

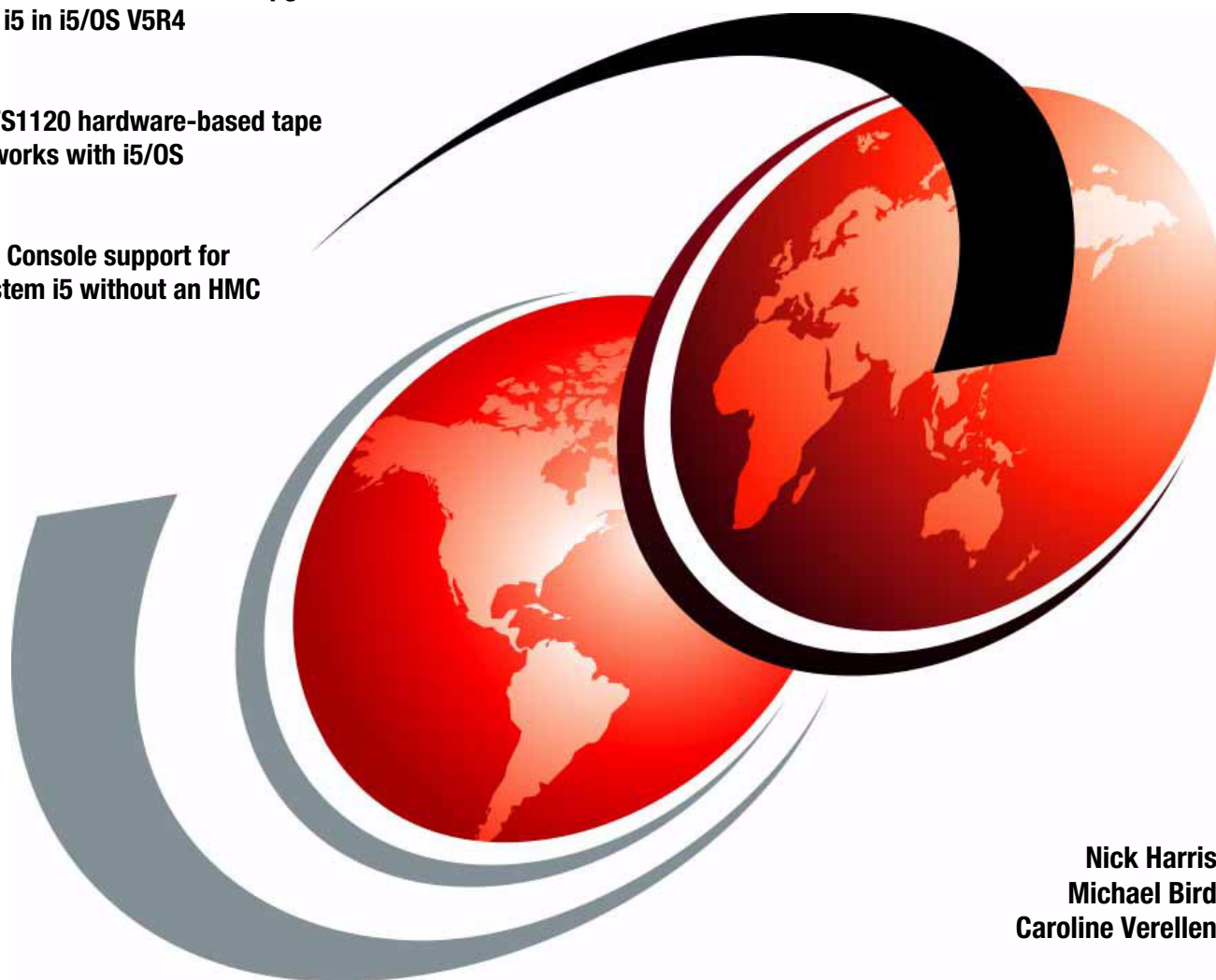
# IBM eServer iSeries Migration

**A Guide to Upgrades and Migrations to IBM System i5**

Understand the considerations for upgrades to  
IBM System i5 in i5/OS V5R4

Learn how TS1120 hardware-based tape  
encryption works with i5/OS

Review Thin Console support for  
low-end System i5 without an HMC



Nick Harris  
Michael Bird  
Caroline Verellen

**Redbooks**





International Technical Support Organization

**IBM eServer iSeries Migration: A Guide to Upgrades  
and Migrations to IBM System i5**

August 2007

**Note:** Before using this information and the product it supports, read the information in “Notices” on page vii.

**Second Edition (August 2007)**

[This edition applies to Version 5, Release 4, Modification 0 of i5/OS.](#)

**© Copyright International Business Machines Corporation 2005, 2007. All rights reserved.**

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

<b>Notices</b> .....	vii
Trademarks .....	viii
<b>Preface</b> .....	ix
The team that wrote this IBM Redbook .....	ix
Become a published author .....	x
Comments welcome .....	x
<b>Chapter 1. Planning for upgrades to System i5 hardware.</b> .....	1
1.1 Planning fundamentals .....	2
1.1.1 Presales planning .....	2
1.1.2 Postsales planning .....	5
1.2 Migration towers and SPD hardware .....	7
1.2.1 SPD features and their replacements .....	7
1.2.2 SPD features that can be converted to PCI .....	12
1.3 Disk migration .....	12
1.3.1 Redundant Array of Independent Disks arrangements .....	13
1.4 Physical planning .....	16
1.5 Linux migration .....	23
1.5.1 Migrating a Linux logical partition from iSeries .....	24
1.6 Windows migration .....	24
1.6.1 Moving the Integrated xSeries Adapter or Integrated xSeries Server from iSeries 8xx to 5xx .....	24
1.7 IBM AIX 5L migration .....	24
1.8 Migration and upgrade check list .....	25
<b>Chapter 2. Migration examples</b> .....	33
2.1 General upgrade considerations .....	34
2.1.1 Side-by-side upgrade and data migration using the side-by-side method .....	35
2.1.2 Data migration using the side-by-side method (source system in the previous release) .....	36
2.1.3 Upgrade using unload/reload .....	37
2.1.4 Upgrade with converted or relocated disks .....	38
2.1.5 Upgrade with load source migration .....	39
2.2 Migration examples .....	40
2.2.1 Model 810 to model 520 (or 525, 550) with no LPAR .....	40
2.2.2 Model 820 with tower to model 520 (525, 550) with no LPAR .....	42
2.2.3 Model 640 to model 520 (or 525, 550) no LPAR .....	43
2.2.4 Model 720 to model 520 (or 525, 550) .....	44
2.2.5 Model 840 to model 570 (system upgrade with no LPAR or Hardware Management Console) .....	45
<b>Chapter 3. System i5 disk at i5/OS V5R4</b> .....	51
3.1 Introducing the System i5 disk technology .....	52
3.2 Disk types (speeds and feeds) .....	52
3.3 Disk packaging .....	52
3.3.1 System i 515, 525, 520, and 550 .....	52
3.3.2 System i 570 .....	52
3.3.3 System i 595 .....	52

3.3.4 I/O expansion . . . . .	52
3.4 Disk protection types . . . . .	53
3.4.1 RAID-5 vs RAID-6 . . . . .	55
3.4.2 Considerations when planning disk protection . . . . .	56
3.4.3 Migrating to RAID-6 from unprotected disk with iSeries Navigator . . . . .	64
3.4.4 Migrating to RAID-6 from unprotected disk using dedicated service tools . . . . .	66
3.4.5 Migrating to RAID-6 from unprotected disk using system service tools . . . . .	68
3.4.6 Migrating to RAID-6 from mirrored . . . . .	68
3.4.7 Migrating to RAID-6 from RAID-5 protected . . . . .	68
3.5 Load source migration . . . . .	69
3.5.1 Considerations for load source migration . . . . .	69
3.5.2 Load source migration: No disk protection . . . . .	70
3.5.3 Load source migration: Mirrored system . . . . .	75
3.5.4 Load source migration: RAID system . . . . .	85
3.5.5 RAID-5 arrangement on Peripheral Component Interconnect-X I/O adapters . . . . .	86
<b>Chapter 4. System i5 consoles in i5/OS V5R4 . . . . .</b>	<b>89</b>
4.1 Introduction to the consoles on System i5 servers . . . . .	90
4.1.1 Twinax console . . . . .	90
4.1.2 Operations console (direct-attached or LAN-attached) . . . . .	90
4.1.3 The Hardware Management Console . . . . .	90
4.2 Thin Console . . . . .	97
4.2.1 Thin Console installation . . . . .	97
4.2.2 Specifications . . . . .	97
4.2.3 Thin Console 5250 emulation screen . . . . .	98
4.2.4 Neoware Connection Manager . . . . .	101
4.2.5 Physical installation and cabling . . . . .	102
4.2.6 Customization settings . . . . .	110
4.2.7 Maintenance . . . . .	119
4.2.8 Backup/recovery and availability considerations . . . . .	123
4.2.9 Troubleshooting . . . . .	124
4.3 Console card locations . . . . .	126
4.3.1 Designated slots for models 5xx (V5R3) . . . . .	126
4.3.2 i5/OS V5R3M5 and V5R4 (new Smart IOA plus+ models) . . . . .	127
4.4 Changing the console type . . . . .	127
4.4.1 Using the console service functions (65+21) . . . . .	128
<b>Chapter 5. i5/OS V5R4 software . . . . .</b>	<b>129</b>
5.1 i5/OS V5R4 software requirements and information . . . . .	130
5.1.1 i5/OS V5R4 informational authorized program analysis report and PSPs . . . . .	130
5.1.2 Required software . . . . .	131
5.1.3 AS/400 models not supported in i5/OS V5R4 . . . . .	131
5.1.4 License agreements . . . . .	131
5.2 i5/OS V5R4 software upgrade paths . . . . .	131
5.3 Interoperability with the existing systems . . . . .	132
5.4 i5/OS V5R4 software upgrade . . . . .	132
<b>Chapter 6. Tape data encryption in i5/OS V5R4 . . . . .</b>	<b>137</b>
6.1 Using the Encryption Key Manager and TS1120 tape drive . . . . .	138
6.1.1 Encryption methods . . . . .	138
6.1.2 Encryption components . . . . .	139
6.1.3 Planning for tape encryption . . . . .	140
6.1.4 Backup and recovery considerations with Encryption Key Manager . . . . .	140
6.1.5 Encryption Key Manager server on a PC . . . . .	142

6.1.6 Creating a keystore . . . . .	148
6.2 Creating keys in your keystore . . . . .	151
6.2.1 Creating a self-signed key . . . . .	151
6.2.2 Creating a certificate request . . . . .	153
6.2.3 Importing keys from another keystore . . . . .	156
6.3 Configuring Encryption Key Manager . . . . .	159
6.3.1 Editing the .properties file . . . . .	159
6.3.2 Starting the EKM Admin Console (command prompt) . . . . .	162
6.3.3 Starting and stopping the EKM server . . . . .	163
6.3.4 Adding tape drives to the EKM drive table . . . . .	163
6.4 Encryption Key Manager on i5/OS . . . . .	164
6.4.1 Software requirements . . . . .	164
6.4.2 Installing the unrestricted policy files. . . . .	164
6.4.3 Installing the Encryption Key Manager .jar and sample configuration file. . . . .	165
6.4.4 Installing Digital Certificate Manager. . . . .	165
6.5 Creating a keystore in DCM . . . . .	167
6.5.1 Creating keys . . . . .	170
6.5.2 Creating a private/public key pair in your keystore . . . . .	173
6.5.3 Importing a key into the keystore . . . . .	175
6.5.4 Creating a local Certificate Authority-signed key in your keystore . . . . .	176
6.6 Configuring Encryption Key Manager . . . . .	180
6.6.1 Editing the .properties file . . . . .	180
6.6.2 Starting the EKM Admin Console (command prompt) . . . . .	181
6.6.3 Starting and stopping the EKM server . . . . .	183
6.6.4 Adding the tape drives to the EKM drive table . . . . .	183
6.7 Configuring your TS1120 tape drive for encryption. . . . .	184
6.7.1 Defining the keystores to be used by the TS3500 . . . . .	184
6.7.2 Enabling your tape drive for encryption. . . . .	188
6.7.3 Setting up a scratch encryption policy. . . . .	190
6.7.4 Rekeying an encrypted cartridge for use by another company. . . . .	193
<b>Related publications . . . . .</b>	<b>195</b>
IBM Redbooks . . . . .	195
Other publications . . . . .	195
Online resources . . . . .	195
How to get IBM Redbooks . . . . .	196
Help from IBM . . . . .	196
<b>Index . . . . .</b>	<b>197</b>





# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.


This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

## COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

# Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX 5L™	Lotus®	System p™
AIX®	OS/400®	System x™
AS/400e™	PowerPC®	System Storage™
AS/400®	POWER™	Tivoli®
Domino®	POWER5™	TotalStorage®
eServer™	Redbooks®	WebSphere®
IBM®	Redbooks (logo)  ®	xSeries®
iSeries®	System i™	zSeries®
i5/OS®	System i5™	1350™

The following terms are trademarks of other companies:

Java, JDK, JRE, JVM, J2SE, Sun Java, Ultra, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft., Windows Server., Windows., and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Itanium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

# Preface

Planning an upgrade from an existing IBM® AS/400e™ or IBM eServer™ iSeries® server to a new model IBM System i5™ can range from a very simple disk migration to a complex task involving many components and OS upgrade steps. This IBM Redbook discusses the various topics that are involved in migrating to the new Peripheral Component Interconnect-X (PCI-X) and IBM POWER5™ processor technology.

Upgrade scenarios are included to assist your planning.

IBM i5/OS® V5R4 contains additional components, functions, and features, which this book discusses. The new features include the new Thin Console support for the IBM System i5 low-end system. This book also discusses the new hardware-based tape encryption that is available with i5/OS V5R4 and the IBM TotalStorage® TS1120 tape drive.

Whether you are an IBM Field Technical Support Specialist, business partner, or client, this book offers the guidance you require to plan your upgrade or migration to a new IBM System i5 system.

## The team that wrote this IBM Redbook

This book was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Poughkeepsie Center.

**Nick Harris** is a Consulting IT Specialist for the IBM System i5 and works in the Rochester Executive Briefing Center. He spent the past nine years at the ITSO's Rochester Center. He specializes in logical partition (LPAR), iSeries hardware and software, external disk, Integrated IBM xSeries® Server for iSeries, and Linux®. He has written and taught IBM classes worldwide on IBM System i5, iSeries, and IBM AS/400® system design and server consolidation. He spent 13 years in the United Kingdom (UK) AS/400 Business, and has experience in S/36, S/38, AS/400, and iSeries servers. You can contact him at [niharris@us.ibm.com](mailto:niharris@us.ibm.com).

**Michael Bird** is a freelance IT consultant in the UK. He has more than 20 years of experience in IT. He worked for IBM for 10 years as a Customer Engineer (CE) and in the AS/400 Support Centre. His areas of expertise include iSeries hardware migration, LPAR configuration, disaster recovery, communications and networking. He is a certified iSeries Technical Expert, Cisco Certified Network Associate (CCNA), Cisco Certified Design Associate (CCDA), and Microsoft® Certified Systems Engineer (MCSE). You can contact him at [MBTechnology@BTClick.com](mailto:MBTechnology@BTClick.com).

**Caroline Verellen** is a Backup Continuity and Recovery Specialist working for IBM Global Services in Belgium and the Benelux area. She has spent five years at System i5 software support, specializing in System/Backup/Recovery, and three years at IBM Backup Continuity and Recovery Services as System Engineer, i5, where Caroline consults with System i5 customers on disaster recovery plans and recovery procedures, managed and housed high availability systems, and upgrading hardware/software (HW/SW) in a Business Continuity and Recovery Services (BC&RS) environment. You can contact her at [Caroline\\_Verellen@be.ibm.com](mailto:Caroline_Verellen@be.ibm.com).

Thanks to the following people for their contributions to this project:

Sue Baker  
Pat Cawley  
Joe Gibbons  
Duane Grosz  
Mike Konkel  
Scott Maxson  
Mark Olson  
Brian Podrow  
Barb Smith  
Tracy Smith  
Allyn Walsh  
Geoff Warren  
Larry Youngren  
IBM Rochester

John Morganti  
IBM Austin

Carla Ruhl  
Thai Tran  
IBM Tucson

Tom Benjamin  
John Peck  
IBM Endicott

## Become a published author

Join us for a two-week to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will team with IBM technical professionals, Business Partners, and clients.

Your efforts will help increase product acceptance and client satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)

## Comments welcome

Your comments are important to us!

We want our IBM Redbooks® to be as helpful as possible. Send us your comments about this or other IBM Redbooks in one of the following ways:

- Use the online **Contact us** review IBM Redbook form found at:

[ibm.com/redbooks](http://ibm.com/redbooks)

- Send your comments in an e-mail to:

[redbook@us.ibm.com](mailto:redbook@us.ibm.com)

- Mail your comments to:

IBM Corporation, International Technical Support Organization  
Dept. HYTD Mail Station P099  
2455 South Road  
Poughkeepsie, NY 12601-5400





# Planning for upgrades to System i5 hardware

This chapter discusses planning considerations for moving to the IBM System i™ 515, 520, 525, 550, 570, and 595 hardware models.

The introduction of the Hardware Management Console (HMC) and the increasing integration of Linux, AIX®, and Windows® environments into System i servers results in a potentially more complex upgrade process. Subsequently, the planning process requires more attention from all parties involved — the client, the IBM Business Partners, the IBM sales team, and the IBM Customer Engineer — to ensure a successful upgrade with minimal disruption.

## 1.1 Planning fundamentals

Careful planning is an essential step in implementing a successful upgrade. This section deals with an overview of the planning process. This process can be applied to any upgrade.

The planning process has two distinct phases:

- ▶ Presales planning
- ▶ Postsales planning

As a general rule you should review the System i planning Web site at:

<http://www.ibm.com/systems/support/i/planning/>

Also, check the support planning Web site at:

<http://www.ibm.com/systems/support/i/planning/upgrade/index.html>

### 1.1.1 Presales planning

This section discusses the preorder tasks. Whether the order is new or an upgrade, it is recommended that the first configuration planning is performed with the IBM System Planning Tool (SPT). As yet, the SPT does not directly support upgrades, but it can be used to validate the final upgrade configuration. This is the sequence of actions:

1. Importing or re-creating the pre-upgrade configuration
2. Validating the configuration
3. Adding the new logical partition (LPAR) configuration and the new components, which in turn results in the final configuration

A combination of the SPT and the System Plans on the HMC allows the deployment of SPT LPAR configurations. At present, the deployment of upgrades is *not* supported.

#### Overview of the System Planning Tool

The SPT is a tool for designing logically partitioned System i and IBM System p™ environments, and is the replacement for the LPAR Validation Tool (LVT). However, it can also be used for planning and documenting nonpartitioned systems.

The SPT is a browser-based tool that runs on your PC. For download and installation information, refer to Appendix A in *IBM Virtualization Engine TS7700: Tape Virtualization for System z Servers*, SG24-7312.

The graphical user interface (GUI) and the order of operations are quite different from the LVT, but its purpose is the same. The tool has help text and a link to the IBM System Hardware Information Center.

The SPT can be found at the following Web site:

<http://www.ibm.com/servers/eserver/support/tools/systemplanningtool/>

You can design new systems from the existing performance data, from the planned workloads, from the sample systems, and by using the advanced mode that lets you design the system at the component level.

SPT creates a system plan that is saved as a .sysplan file. That system plan may be just one system or it may contain multiple systems, each with a unique system name.



The output of the SPT can be used either to create a report or as an input to the IBM Configurator for e-business (e-Config) for order processing. The report function of the SPT invokes the System Plan Viewer, which has a print option. You will also be able to use the .sysplan file to automatically create and deploy partitions on an HMC.

### ***Downloading the SPT***

As is the case with the LVT, the SPT is available for download from the ibm.com Web site. A subscriber list is used to notify users when a new version is available.

The first time you download the SPT, you must use the full version that includes the required Java™ Virtual Machine (JVM™) code and other support files. To download subsequent versions of the SPT, you can download the update version of the SPT. In either case, when you run the .exe file, an install wizard is initiated to guide you through the installation. An icon for the SPT is placed on your desktop when the installation is complete.

The new SPT is available for download from the ibm.com support Web site:

<http://www-03.ibm.com/servers/eserver/support/tools/systemplanningtool/>

### **IBM Workload Estimator**

The IBM Systems Workload Estimator (WLE) is a Web-based sizing tool for IBM System i, IBM System p, and IBM System x™. Use this tool to size a new system, to size an upgrade to an existing system, or to size a consolidation of several systems. The Workload Estimator enables measurement input to best reflect your current workload, and provides a variety of built-in workloads to reflect your emerging application requirements. Virtualization can be used to yield a more robust solution. The Workload Estimator provides current and growth recommendations for processor, memory, and disk that satisfy the overall client performance requirements.

The tool is currently capable of estimating the computer resources required for IBM Lotus® Domino®, IBM WebSphere® Commerce, IBM WebSphere, Web serving, and traditional workloads. The Workload Estimator projects the most current System i5 server models that meet the capacity requirements within the CPU % utilization objectives. Workload Estimator can be used alone or in conjunction with the System Planning Tool.

### ***Workload Estimator download Web site***

Download the Workload Estimator from:

<http://www.ibm.com/jct01004c/systems/support/tools/estimator/index.html>

Figure 1-1 on page 4 shows the Workload Estimator home page. Use the link shown in the browser window to start the download, and follow the on-screen instructions.

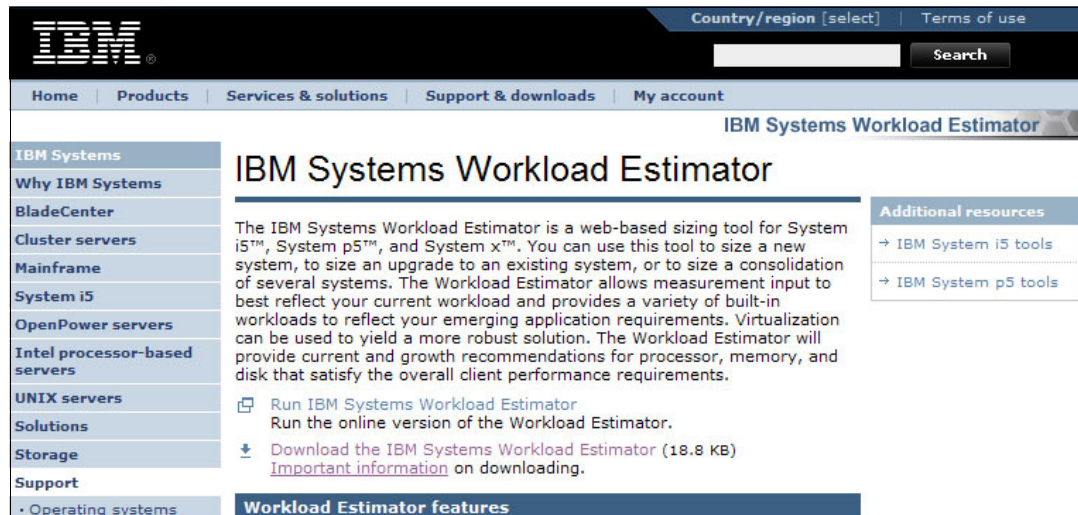


Figure 1-1 WLE download page

## Solution proposal

By discussing the client's existing server configuration and their requirements, the IBM Sales Representative or IBM Business Partner formulates a complete proposal. During this phase of the project, the baseline information about the client environment must be gathered.

During the solution proposal, use the Workload Estimator or one of the System i capacity planning tools to establish the size and the capacity of the System i server. For more information about the Workload Estimator, refer to the following Web site:

<http://www-304.ibm.com/jct01004c/systems/support/tools/estimator/index.html>

You must also review the information in the IBM Systems Hardware Information Center. Much of the hardware planning information for both IBM System i5 and IBM System p5 servers is now available in the Hardware Information Center at:

<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp>

The IBM Prerequisite Web site provides you with compatibility information for hardware features. This tool helps you to plan a successful system upgrade by providing you with the prerequisite information for the features you currently have or plan to add to your system:

[http://www-912.ibm.com/e\\_dir/eServerPrereq.nsf](http://www-912.ibm.com/e_dir/eServerPrereq.nsf)

If you are working with an existing System i server that has an HMC at V5R2, you can use the System Plan function to gather hardware and partition information that can be utilized for the creation of your SPT model. You will not be able to deploy the upgrade system plan unless the upgrade is to just add hardware for an additional partition. For more information about the System Planning Tool and the System Plan function of the HMC, refer to:

<http://www.ibm.com/servers/eserver/support/tools/systemplanningtool/>

You can also refer to the *LPAR Simplification Tools Handbook*, SG24-7231.

## Initial e-Config output

The initial server design can be output from e-Config, which enables IBM Sales Representatives or IBM Business Partners to design a possible new server or upgrade solution. This initial plan might be an iterative process as the alternatives for components and availability options are considered.

The e-Config output also leads to a discussion of whether the server configuration is suitable in terms of commercial processing workload (CPW), main storage, auxiliary storage, LAN/WAN connectivity, availability requirements, console requirements, physical dimensions, and power and cooling requirements.

During this consideration phase, both the system and application software must be considered. The new IBM System i5 models require IBM i5/OS V5R3 or later, depending on the model (that is, whether the server is partitioned). All of the logical partitions must also be at i5/OS V5R3 or later. Some functions require i5/OS V5R3M5 or i5/OS V5R4, such as initial program load (IPL) system across system area network (SAN) or input/output processor-less (IOP-less) adapter cards.

### **Initial plan and schedule**

At this stage, the client looks at the issues described until now and, along with application considerations, at whether the proposed solution is worth pursuing. LPAR, clustering, and high availability solutions might form a part of the planning at this stage.

The result of these activities is an initial plan and schedule for the upgrade. Physical planning is one part of the process that is performed at this stage (dimensions, power and cooling requirements, LAN/WAN connectivity, and so on). The plan must identify all activities that are required to move from the client's current server to the proposed server; for example, a software upgrade is most likely to be required.

Depending on the vintage of the current server, it is possible that there is hardware to be removed from the current server prior to the main upgrade, and so on. This results in a multipart upgrade where hardware is removed or added at different stages. The final stage is to replace the existing central electronic complex (CEC) with a new one and any hardware not already installed. No SPD (system product division) hardware may be attached to a System i5.

### **Final e-Config output and order**

Subsequent to the activities described until now, the solution proposal might require refinement. This refinement is input into the e-Config and the upgrade order is finalized.

### **Order and schedule**

Place the order and move to the postsales planning stage.

## **1.1.2 Postsales planning**

This section involves planning the actual upgrade procedures.

The final e-Config output and the client requirements resulting from the presales phase give rise to a unique timeline and task list for this client's upgrade. The IBM-recommended upgrade flow is outlined. Although it is tempting to merge many of these tasks into a much shorter timeline, good project management practice involves minimizing the number of changes performed at any given time. This minimizes the possibility of failure and ensures easier problem resolution, if necessary.

### **Preparation for feature upgrade**

If the client has hardware that is not supported at the target release of IBM OS/400®, steps must be taken to remove this hardware and, if required, replace it with functionally equivalent hardware.

Planning is required to ensure the correct positioning and functionality of this hardware.

A readiness check is advised before proceeding. If there are complex or advanced components in the configuration, the IBM Sales Representative or IBM Business Partner can run a systems assurance review. This is a checkpoint to ensure that certain advanced options have been adequately considered.

### ***Feature upgrade***

Feature upgrade can be performed by the client, an IBM Service Representative, or an IBM Business Partner, depending on the features being replaced. Instructions are included with the hardware. A feature upgrade can be as small as adding an Ethernet adapter or using concurrent maintenance, or as large as adding multiple expansion towers with many disks and adapters. Certain features might also require an upgrade to i5/OS V5R3 before they can be installed.

### **Resource management and preparation for software upgrade**

After the first feature upgrade, the client must perform some hardware resource management, cleanup work, and testing to ensure that all required functions are working correctly. Also, in this stage, the preparation work for the OS/400 software upgrade is performed. A readiness check is recommended before proceeding.

### ***Software upgrade***

The i5/OS upgrade is a client responsibility, unless it is contracted to IBM or an IBM Business Partner. A test environment must be available to create a version of the system and its applications. Ideally, this would be on an i5 server to ensure that there are no hardware interactions that could hamper the actual upgrade. However, it is possible to test the i5/OS V5R3 software on any older iSeries server that supports V5R3. This could be a 7xx or 8xx model. i5/OS V5R4 can also be installed on 5xx or 8xx models if the system or LPAR has a 17 GB load source drive.

This enables system and application function testing, but not volume testing. If the system that is to be migrated has critical applications, consider making a trip to the IBM Rochester Benchmark Center. Here, you can test both the function and the capacity on an i5 server, even before you place an order. The Benchmark Center is a fee-based offering. For more information, refer to the following Web site:

<http://www.ibm.com/servers/eserver/iseries/benchmark/cbc/index.html>

We appreciate the cost involved, but it is often well worth the investment. For example, if you are planning to spend \$150,000 on a server, it would be a small investment to spend \$15k - \$20k on a benchmark test. You will also benefit from access to the new software and hardware, plus getting the additional benefit of skills transfer to key client staff.

### **Stabilization and preparation for the server model upgrade**

After the OS/400 upgrade, the client must allow the server the time to stabilize at the new release, allowing time for any OS/400 or application issues to be identified and resolved before proceeding further.

During this stage, the client also plans the upgrade to the server. Physical planning (position, weight, power and cooling requirements, and so on) is performed. LPAR configuration might require resources to be moved from their shipped location. Disk migration might result in data migration and disk reconfiguration prior to upgrade. The client must save the LPAR configuration from the iSeries Navigator to a diskette for later loading on the HMC or manually keying in the LPAR configuration into the HMC.

A readiness check is required before proceeding further.

## System model upgrade

The client hands over all of this information to the IBM customer engineer (CE), who performs the miscellaneous equipment specification (MES) upgrade. It is vital that the client has actually performed the critical planning stages outlined earlier. The client might begin to set up the HMC in a stand-alone setting (that is, not plugged into the server).

## Resource management and production

After the new server is powered on, the CE connects the HMC. The client loads the saved LPAR configuration from the diskette, using the LPAR migration utility. The CE applies the partition profiles created by the LPAR migration tool to the server where the partitions are created. The CE then returns the server to the client, who performs hardware resource management activities and tests the server before moving to production.

Any new applications are installed at this stage by the client, an IBM Business Partner, or an application vendor.

## 1.2 Migration towers and SPD hardware

This section discusses the migration towers and SPD hardware that might already exist on the 8xx server to be upgraded. These hardware resources are not supported on the new 5xx servers. The client must prepare a replacement strategy.

A migration tower (#5034, #5035, or #5077) is essentially a 7xx installed system unit converted to a tower. This conversion enables the client to retain some of their existing SPD and older Peripheral Component Interconnect (PCI) hardware upon upgrade to a model 8xx (models 810, 825, 870, and 890 only), thus leveraging their existing investment. When converted into a migration tower, the new tower connects to the system unit using a high-speed link (HSL). The existing SPD towers can be attached through a migration tower.

SPD hardware, including migration towers, is not supported on iSeries model 5xx. As part of the planning process, you must remove all existing SPD hardware before or during the upgrade, and sufficient resources must be available in the upgraded system to perform the function of the removed hardware. When planning the change from SPD to PCI features, some PCI replacements have differing functions and requirements that you might have to address; for example, the fax adaptor requires reconfiguring, and might have implications for any fax applications you use. Some resources have no PCI alternative, for example, #6141 American Standard Code for Information Interchange (ASCII) adaptor and #2644 channel attach tape IOP. For most tape input/output adapter (IOA) replacements, you have to change the cable or interposer that is used to connect the tape drive to the Small Computer System Interface (SCSI).

It is possible to upgrade #5065 and #5066 towers to their PCI equivalents (#5074 and #5079 respectively), which gives an upgrade path from SPD and migration towers. That is, convert SPD hardware to the PCI equivalent, install in #5065/#5066 towers, and then upgrade these towers as part of the main upgrade process.

### 1.2.1 SPD features and their replacements

Table 1-1 on page 8 lists the existing SPD features that you might have and their possible PCI replacements.

Table 1-1 SPD features and towers that must be replaced

SPD feature code	Card description and properties	Suggested replacement PCI feature	Card description and properties
2686	Optical link processor (266 Mbps). Used for attaching #5044. Each #2686 supports a maximum of one #5044.	HSL port	
2688	Optical link processor (1063 Mbps). Used for attaching #5065, #5072, #5073, #5082, and #5083 expansion towers. Each #2688 supports a maximum of two #50xx towers.	HSL port	
2695	Optical bus adapter. Allows for the addition of up to three #2686 or #2688 optical link processors in any combination.	HSL port	
5044	System unit expansion rack. This is a 12 SPD I/O card slot cage in a rack enclosure.	5094, 5294, 5095, 5075, 5074, or 5079 <sup>1</sup>	PCI expansion tower <sup>1</sup>
5052 and 5058	Storage expansion unit. Provides space for up to 16 disk units.	5094, 5294, 5095, 5075, 5074, or 5079 <sup>1</sup>	PCI expansion tower <sup>1</sup>
5055 and 5057	Storage expansion unit. Provides space for up to eight to 16 disk units.	5094, 5294, 5095, 5075, 5074, or 5079 <sup>1</sup>	PCI expansion tower <sup>1</sup>
5072 and 5073	1063 Mbps system unit expansion tower. Provides an additional bus.	5094, 5294, 5095, 5075, 5074, or 5079 <sup>1</sup>	PCI expansion tower <sup>1</sup>
5082 and 5083	1063 Mbps storage expansion tower. Provides a direct access storage device (DASD) tower for adding up to 16 disk units.	5075, 5074, or 5079 <sup>1</sup>	PCI expansion tower <sup>1</sup>
2629	LAN/WAN/Workstation IOP. This supports up to three LAN/WAN/Workstation IOAs.	2843, 9943, or 2824 <sup>2</sup>	PCI I/O processor that drives PCI IOA adapters
6050, 6140, and 6180	Twinaxial workstation controller. One 8-port attachment is provided to support up to 40 twinaxial devices.	2746 <sup>2</sup> /4746	The twinaxial workstation IOA provides support for up to 40 active twinaxial displays and printer addresses.
6141 and 6142	ASCII workstation controller. This workstation controller supports up to six ASCII devices.	N/A	
2605	Integrated Services Digital Network (ISDN) basic rate adapter	2745 <sup>2</sup> /4745 <sup>3</sup>	#4745 supports up to two multiple protocol communications ports <sup>2</sup>
2609	Electronic Industries Association (EIA) 232/V.24 two-line adapter	2745 <sup>2</sup> /4745 <sup>3</sup>	#4745 supports up to two multiple protocol communications ports <sup>2</sup>

SPD feature code	Card description and properties	Suggested replacement PCI feature	Card description and properties
2610, 2656, and 2659	X.21 two-line adapter	2745 <sup>2</sup> /4745 <sup>3</sup>	#4745 supports up to two multiple protocol communications ports <sup>2</sup>
2612, 2654, 2655, 2657, and 2658	EIA 232/V.24 two-line adapter	2745 <sup>2</sup> /4745 <sup>3</sup>	#4745 supports up to two multiple protocol communication ports <sup>2</sup>
2613, 6153, and 6173	V.35 one-line adapter	2745 <sup>2</sup> /4745 <sup>3</sup>	#4745 supports up to two multiple protocol communication ports <sup>2</sup>
2614	X.21 one-line adapter	2745 <sup>2</sup> /4745 <sup>3</sup>	#4745 supports up to two multiple protocol communication ports <sup>2</sup>
2620 and 2820	Cryptographic processor	4801	PCI cryptographic coprocessor <sup>3</sup>
2623	Six-line communication controller	2843, 9943, or 2824 <sup>2</sup>	PCI I/O processor that drives PCI IOA adapters
2664	Integrated fax adapter	2761 <sup>2</sup> /4761, 2772, 2773, or 2805	See note 10
2666	High-speed communications adapter	2745 <sup>2</sup> /4745 <sup>3</sup>	#4745 supports up to two multiple protocol communication ports <sup>2</sup>
2699 and 9699	Two-line WAN IOA	2745 <sup>2</sup> /4745 <sup>3</sup>	#4745 supports up to two multiple protocol communication ports <sup>2</sup>
2617 and 6181	Ethernet/Institute of Electrical and Electronics Engineers (IEEE) 802.3 adapter	2838 <sup>2</sup> /4838	PCI 100/10 Mbps Ethernet IOA
2618	Fibre distributed data interface adapter	N/A	
2619, 2626, and 6149	16/4 Mbps token ring adapter	4744	PCI 100/16/4 Mbps token-ring IOA
2665	Shielded twisted-pair distributed data interface adapter	N/A	
2663 and 2668	I/O attachment processor wireless LAN adapter	N/A	
2810	LAN/WAN IOP	2843, 9943, or 2824 <sup>2</sup>	PCI I/O processor that drives PCI IOA adapters
FSIOP <sup>4</sup>	Integrated PC server (IPCS)	2790, 2791, or 2799 <sup>4</sup>	
6616, 6617, and 6618	Integrated PC server	<ul style="list-style-type: none"> <li>▶ 2790/2890-----&gt;</li> <li>▶ 2791/2891-----&gt;</li> <li>▶ 2799/2899 -----&gt;</li> <li>▶ 2792/2892<sup>4</sup>----&gt;</li> </ul>	<ul style="list-style-type: none"> <li>▶ 700 MHz Integrated xSeries</li> <li>▶ 850 MHz Integrated xSeries</li> <li>▶ 1.0 GHz Integrated xSeries</li> <li>▶ 1.6 GHz Integrated xSeries</li> </ul>

SPD feature code	Card description and properties	Suggested replacement PCI feature	Card description and properties
8664 and 8665	Base-shielded twisted-pair distributed data interface adapter	N/A	
1312, 1322, 1325, 1327, 1333, 1334, 1337, 1602, 6605, and 6652	<ul style="list-style-type: none"> <li>▶ One-byte 1.03 GB disk unit</li> <li>▶ Two-byte 1.03 GB disk unit</li> </ul>	<ul style="list-style-type: none"> <li>▶ 4317<sup>5</sup></li> <li>▶ 4318<sup>5</sup></li> <li>▶ 4319<sup>5</sup></li> <li>▶ 4326</li> <li>▶ 4327</li> </ul>	<ul style="list-style-type: none"> <li>▶ 8.58 GB disk unit 10k revolutions per minute (rpm)</li> <li>▶ 17.54 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 15k rpm</li> <li>▶ 70.56 GB disk unit 15k rpm</li> </ul>
1313, 1323, 1326, 1336, 1603, 6606, 6650, 6806, 6906, and 9606	<ul style="list-style-type: none"> <li>▶ One-byte 1.96 GB disk unit</li> <li>▶ Two-byte 1.96 GB disk unit</li> </ul>	<ul style="list-style-type: none"> <li>▶ 4317<sup>5</sup></li> <li>▶ 4318<sup>5</sup></li> <li>▶ 4319<sup>5</sup></li> <li>▶ 4326<sup>5</sup></li> <li>▶ 4327<sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>▶ 8.58 GB disk unit 10k rpm</li> <li>▶ 17.54 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 15k rpm</li> <li>▶ 70.56 GB disk unit 15k rpm</li> </ul>
1327, 1337, 6607, 6807, 6907, 9707, and 9907	Two-byte 4.19 GB disk unit	<ul style="list-style-type: none"> <li>▶ 4317<sup>5</sup></li> <li>▶ 4318<sup>5</sup></li> <li>▶ 4319<sup>5</sup></li> <li>▶ 4326<sup>5</sup></li> <li>▶ 4327<sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>▶ 8.58 GB disk unit 10k rpm</li> <li>▶ 17.54 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 15k rpm</li> <li>▶ 70.56 GB disk unit 15k rpm</li> </ul>
1333, 6713, 6813, 8713, and 8813	Two-byte 8.58 GB disk unit	<ul style="list-style-type: none"> <li>▶ 4317<sup>5</sup></li> <li>▶ 4318<sup>5</sup></li> <li>▶ 4319<sup>5</sup></li> <li>▶ 4326<sup>5</sup></li> <li>▶ 4327<sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>▶ 8.58 GB disk unit 10k rpm</li> <li>▶ 17.54 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 15k rpm</li> <li>▶ 70.56 GB disk unit 15k rpm</li> </ul>
1334, 6714, 6824, 8714, and 8824	Two-byte 17.54 GB disk unit	<ul style="list-style-type: none"> <li>▶ 4318<sup>5</sup></li> <li>▶ 4319<sup>5</sup></li> <li>▶ 4326<sup>5</sup></li> <li>▶ 4327<sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>▶ 17.54 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 10k rpm</li> <li>▶ 35.16 GB disk unit 15k rpm</li> <li>▶ 70.56 GB disk unit 15k rpm</li> </ul>
1349, 1379, and 6368	1.2 GB ¼-inch cartridge tape unit	4482 or 4582 <sup>6</sup>	4 GB ¼-inch cartridge tape unit
1350™, 1380, 6369, 6380, 6381, and 6481	2.5 GB ¼-inch cartridge tape unit	4482 or 4582 <sup>6</sup>	4 GB ¼-inch cartridge tape unit
1355, 6385, and 6485	13 GB ¼-inch cartridge tape unit	4483 or 4583 <sup>7</sup>	16 GB ¼-inch cartridge tape unit
1360, 6390, and 6490	7 GB 8 mm cartridge tape unit	N/A <sup>8</sup>	8 mm cartridges are supported only through external 7208 devices <sup>8</sup>
6325 and 6425	Optional CD-ROM feature	4425 or 4525	CD-ROM device
2621	Removable media device attachment	2729 <sup>2</sup> or 2749	PCI Ultra™ magnetic media controller
2624	Storage device controller	<ul style="list-style-type: none"> <li>▶ 2748<sup>2</sup>, 4748, 9748<sup>9</sup>,</li> <li>▶ 2778<sup>2</sup>, 4778, or 9778<sup>9</sup></li> </ul>	PCI Redundant Array of Independent Disks (RAID) disk unit controller



SPD feature code	Card description and properties	Suggested replacement PCI feature	Card description and properties
2644	34xx magnetic tape subsystem attachment	N/A	All the devices that are attached to the 2644 IOP are not supported on V5R2.
6112	Magnetic storage device controller	N/A	All the devices that are attached to the 6112 IOP are not supported on V5R2.
6146	Diskette adapter	N/A	All the devices that are attached to the 6146 IOP are not supported on V5R2.
6500	DASD controller	N/A	All the devices that are attached to the 6500 IOP are not supported on V5R2.
6501	Tape/Disk device controller	<ul style="list-style-type: none"> <li>▶ 2729<sup>2</sup> or 2749</li> <li>▶ 2765<sup>11</sup> or 2766<sup>11</sup></li> </ul>	PCI magnetic media controller Fibre Channel (FC) tape and disk controllers
6502, 6512, 6530, 6532, and 6533	RAID disk unit controller	<ul style="list-style-type: none"> <li>▶ 2748<sup>2</sup>, 4748, or 9748<sup>9</sup></li> <li>▶ 2778<sup>2</sup>, 4778 or 9778<sup>9</sup>,</li> <li>▶ 2757<sup>9</sup> or 2782<sup>9</sup></li> </ul>	PCI RAID disk unit controller and PCI-X RAID disk controllers
6513	Internal tape device controller	<ul style="list-style-type: none"> <li>▶ 2748<sup>2</sup>, 4748, or 9748<sup>9</sup></li> <li>▶ 2778<sup>2</sup>, 4778, 9778<sup>9</sup>, 2757<sup>9</sup>, or 2782<sup>9</sup></li> </ul>	PCI RAID disk unit controller and PCI-X RAID disk unit controller
6534	Magnetic media controller	2729 <sup>2</sup> , 2749, or 2768	PCI magnetic media controller

1: In contrast to SPD towers that have either disk space or IOA/IOP slots and limited disk space, HSL towers feature IOP/IOA slots and disk slots in greater quantity than the existing SPD towers. Therefore, depending on the type of SPD towers you are replacing, you have multiple choices for HSL towers.

2: If you are planning on migrating SPD features and towers to 5065 or 5066 before doing an upgrade to an 8xx system, you must use the SPD/PCI features that can reside only in 5065 or 5066 towers.

3: #2745/4745 support up to two multiple protocol communications ports when one or two (in any combination) of the following cables are attached:

- #0348 V.24/EIA232 20 ft PCI cable
- #0349 V.24/EIA232 50 ft PCI cable
- #0353 V.35 20 ft PCI cable
- #0354 V.35 50 ft PCI cable
- #0355 V.35 80 ft PCI cable
- #0356 V.36 20 ft PCI cable
- #0358 V.36 150 ft PCI cable
- #0359 X.21 20 ft PCI cable
- #0360 X.21 50 ft PCI cable
- #0365 V.24/EIA232 80 ft PCI cable
- #0367 Operations Console Cable

4: The Integrated PC Server (IPCS) (earlier known as FSIOP) might be shown as feature #6517, #6518, #6519, #6526, #6527, #6528, or #6529. All FSIOP and 6616 IPCS are no longer supported on V5R1. If you are using an 6617 or 6618 IPCS and planning on moving from SPD

to PCI, the 2790/2890, 2791, 2891, 2799/2899, and 2792/2892 replacement Integrated xSeries Server can only reside in 5074, 5075, or 5079 towers, 270, or 8xx systems. (Some Integrated xSeries Servers are model-dependant.) The new Enterprise Edition Servers ship with an Integrated IBM eServer zSeries® including 9792. There are also Windows considerations to be met when upgrading an Integrated PC Server.

5: All 1.03 GB, 1.96 GB, and 4.19 GB disks are not supported in any 270, 8xx servers, or 5065/5066, 5074/5079/5075, or 5094/5294/5095 towers.

6: 1.2 GB and 2.5 GB ¼-inch cartridges can be read/write on 4482/4582 4 GB ¼-inch cartridge tape units.

7: 13 GB ¼-inch cartridge can be read/write on a 4483/4583 16 GB ¼-inch cartridge tape unit.

8: Internal 8 mm cartridge tape units are no longer supported on 270 or 8xx systems. The alternative is to use an external 7208 tape device.

9: FC2748/4748/9748 are supported by V4R5/V5R1. FC2778/4778/9778 are supported by V5R1 and V5R2. FC2757 and 2782 are supported by V5R2 (February 2003 level).

10: There are numerous fax options for PCI alternatives to the SPD 2664 Integrated FAX Adapter. Refer to the system handbook for alternatives.

11: If the 6501 is being used to attach to an external tape/disk device, it is common for this adapter to be replaced with a 2765 Fibre Channel Tape Adapter or a 2766 Fibre Channel Disk Adapter.

## 1.2.2 SPD features that can be converted to PCI

Table 1-2 shows the SPD features (disks and towers) that can be converted to PCI.

**Note:** The client must check the cost of migrating, for example, disks, against the cost of new drives with faster and higher capacities.

Table 1-2 LSPD features that can be converted to PCI/HSL

SPD features/ towers	Description	PCI/HSL feature conversion	How to convert them to PCI/HSL	PCI tower that will support them
6717, 6817, 8617, and 8817	8.58 GB disk unit 10k rpm	4317	Request for price quotation (RPQ) 847102 or through the configurator	5065, 5066, <sup>1</sup> 5074, and 5079
6718, 6818 8618, and 8818	17.54 GB disk unit 10k rpm	4318	RPQ 847102 or through the configurator	5065, 5066, <sup>1</sup> 5074, and 5079
5065	Storage/PCI expansion unit	5074	Through the configurator	
5066	1.8 m Storage/PCI expansion unit	5079	Through the configurator	

1: If you are adding a new disk to an installed 8xx system, it is recommended that you also take advantage of the situation to convert the installed 10k rpm disk to 5065 or 5066 towers.

## 1.3 Disk migration

Disk migration to new hardware might have considerable cost savings above the purchase of new disks. However, great care must be taken when planning the movement of disks.

Consider the following factors:

- ▶ Disks with capacity less than 8 GB are not supported.
- ▶ Disks of speeds less than 10k rpm are not supported.
- ▶ i5/OS V5R4 requires any load source drive to be at least 17 GB.
- ▶ Disks that are RAID protected can only be moved where the RAID set is maintained.

All disks that do not meet the first two conditions must be removed before or during the upgrade. In the case of an upgrade to i5/OS V5R4, the load source drive must be removed before the upgrade.

Special care must be taken to ensure the fourth criteria, where the RAID sets span more disks than can be physically placed on an IOP; for example, earlier expansion towers had disks in sets of 16 disks (usually two RAID sets). However, because a #5074 has disks in a set of 15 disks, one disk must be removed from the configuration and from its RAID set prior to moving the disks as a set to the #5074.

The new System i5 has fewer internal disk slots in the CEC than most 8xx servers. Therefore, the disks might have to be rearranged to enable RAID sets to be retained, and to have disks to fit in the CEC.

### 1.3.1 Redundant Array of Independent Disks arrangements

In i5/OS V5R4, RAID 6 capability has been introduced for some disk adapters. The client must still choose between RAID 5 or RAID 6 when the disk drives are added into the configuration. For a more detailed discussion of RAID 6, refer to Chapter 3, “System i5 disk at i5/OS V5R4” on page 51.

#### iSeries Navigator

The iSeries Navigator provides an alternative graphical view of the disk drives. This helps you identify the exact location of a drive from a graphical representation. The graphics truly represent the actual position of a drive unit in a tower. To access the graphical view, perform the following tasks:

1. From the iSeries Navigator main window, expand **Configuration and Service** (Figure 1-2).

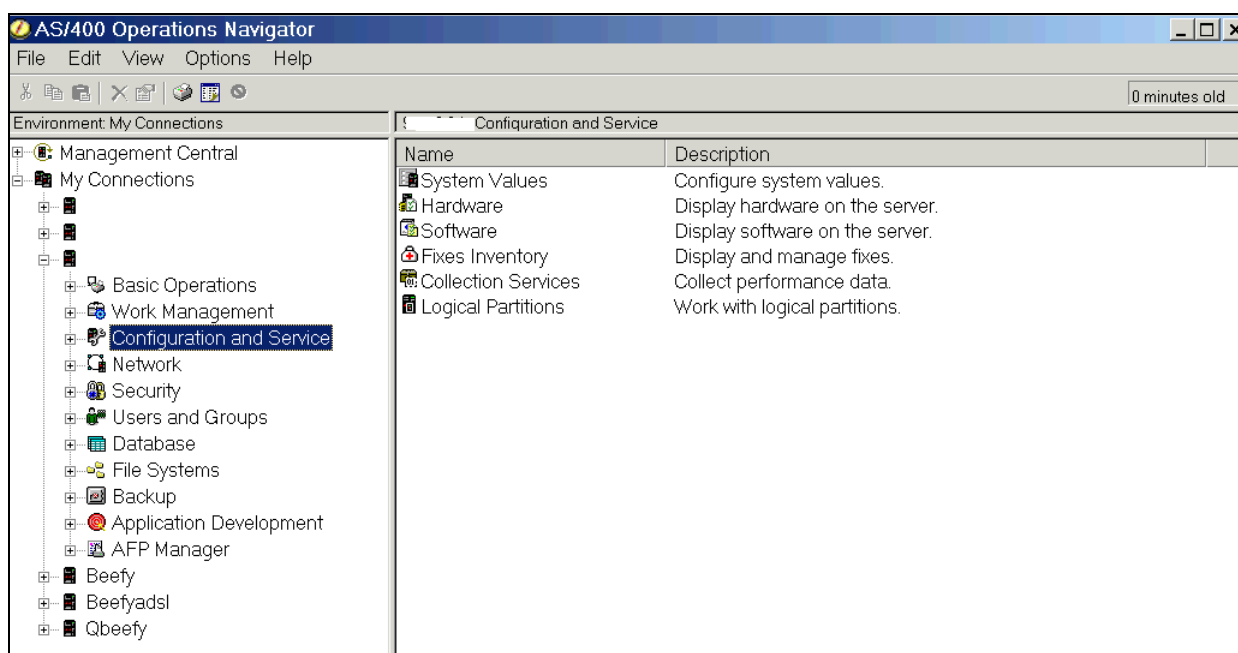


Figure 1-2 iSeries Navigator: Configuration and Service

2. In the right-hand panel, expand **Hardware**.
3. Expand **Disks Units**.
4. You will be asked for a service tools ID and password when you select a resource.

**Notes:** Dedicated and System Service Tool IDs and passwords are *not* the same as the OS/400 user profiles and IDs.

Starting with OS/400 V5R1, service tool passwords are case-sensitive. You may also define multiple IDs, which may also have varying authority levels.

If you forget or disable your service tool IDs, they can be reset by using the command CHGDSTPWD from an OS/400 command line, using the Security Officer profile.

5. Figure 1-3 shows the four options that are available to you:

- All Disks: This provides a list of all the disks on the system.
- By Location: This provides a list of disks by tower. Right-click one of the towers to view its serial number and frame ID. This can be compared to the frame ID displayed on the tower itself.
- Disk Pools: This enables you to view a list of disks according to auxiliary storage pool (ASP).
- Nonconfigured Disks: This provides a list of disks found on the system, but have not yet been added to an ASP.

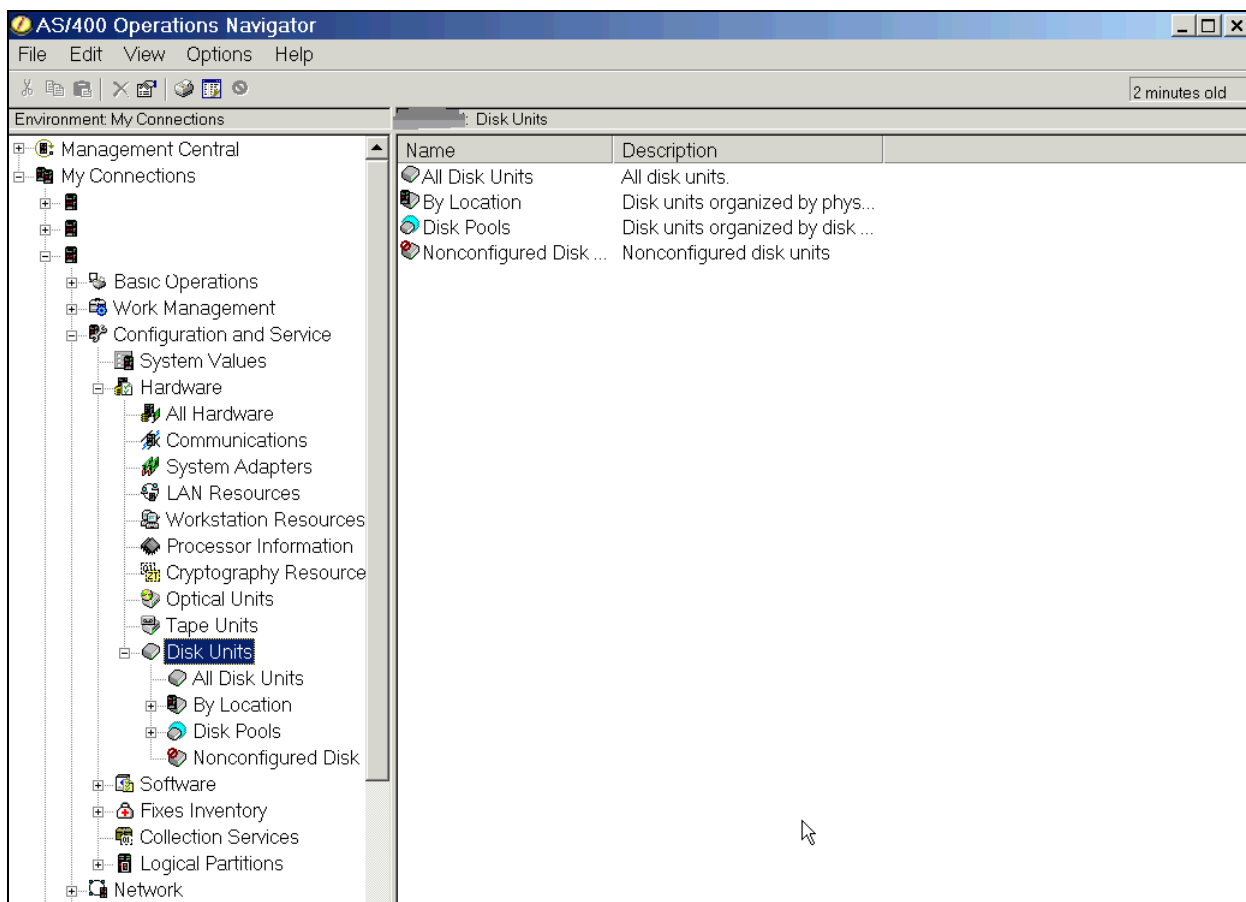


Figure 1-3 Configuration and Service: Disks

6. Right-click **By Location** and select **Graphical view**.

The disk graphics are “hot” and show where the disk is situated on the system, so that it can be identified easily. Right-click one of the disks and select **Properties** to see more

information about the disks, such as serial number, location, percent full, percent busy, and, most important, the unit number required by STRASPBAL. Figure 1-4 shows the pop-ups.

To review the details in each frame, right-click the frame and select **Properties**. This shows the serial number and frame ID for each frame. The frame ID information can be compared to the LED on each frame, so that you can identify each frame.

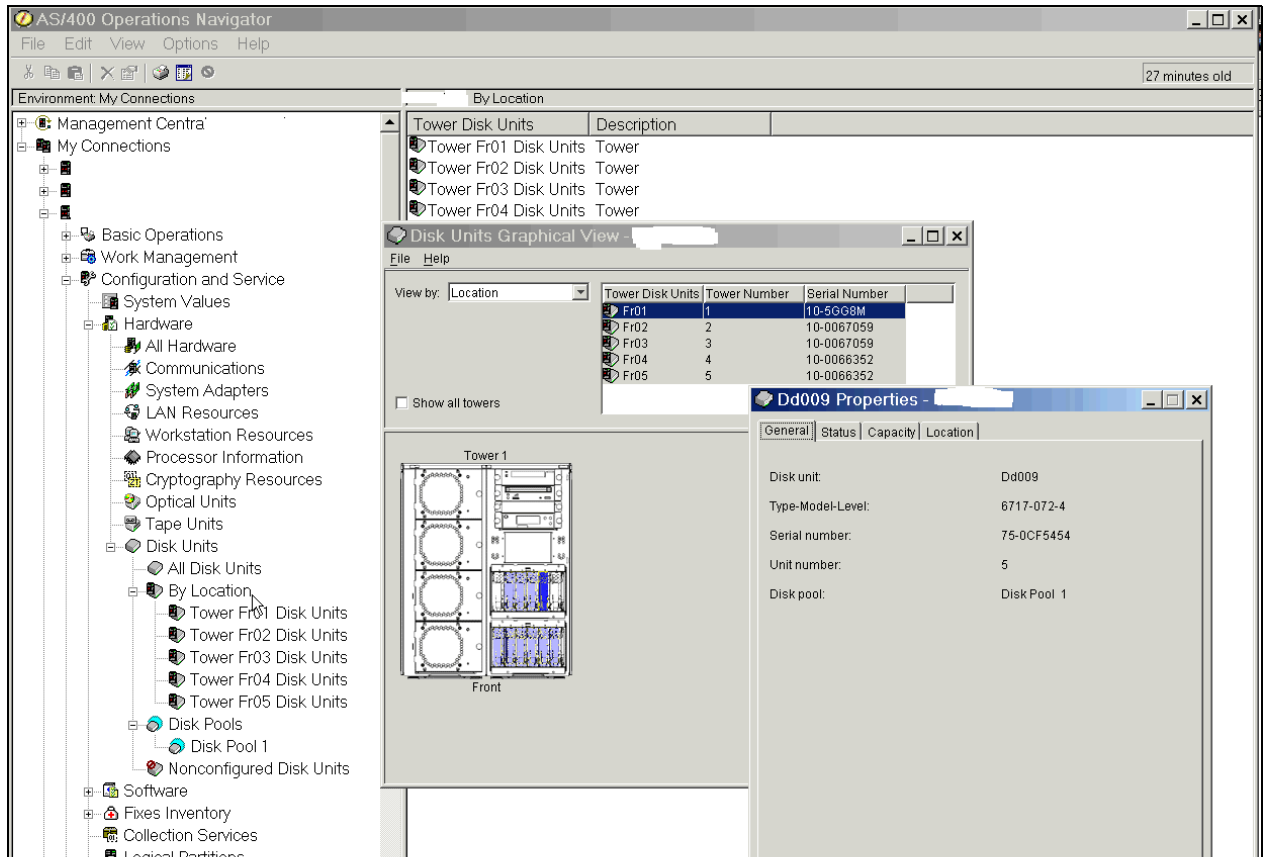


Figure 1-4 iSeries Navigator: Disk properties

You now have sufficient information to identify the disks marked for removal.

## A System Rack List

A System Rack List provides useful documentation about the hardware contained in your system, including information such as hardware features, locations, and serial numbers of each resource on the system.

To obtain a System Rack List, perform the following tasks:

1. Type STRSST in the command line. The System Services Tools sign-in window is displayed. Enter your user ID and password.

**Notes:** Dedicated and System Service Tool IDs and passwords are not the same as the OS/400 user profiles and IDs.

Starting in V5R1 service tools passwords are case sensitive; you may also define multiple IDs.

If you forget or disable your service tools IDs, they can be reset with the command CHGDSTPWD from an OS/400 command line, using the Security Officer profile.

2. In the System Service Tools main menu, select:
  - a. Type 1 - Start a service tool
  - b. Type 7 - Hardware Service Manager
  - c. Select F6 - Print configuration
3. Some print format options are presented. If your printer allows it, use 132 characters-wide, and press Enter.
4. A spool file is submitted to the service printer. Usually, this is a QPRINT output queue.

You now have a printout of the hardware on your system that can be used to help identify the disk units on your system and their location.

## 1.4 Physical planning

For detailed specifications, refer to the physical planning guide or the physical planning section of the IBM eServer Hardware Information Center on the Web at:

<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp>

### The i520/i550 physical layout

Figure 1-5 shows the plan view of the i520/i550. Do not let this system intimidate you. It is very similar to the layout of a PC server. There are six Peripheral Component Interconnect-X (PCI-X) card slots and eight memory dual inline memory module (DIMM) slots. The side panel of the i520 can be removed to install and remove features. The i520 is available as a desk-side unit or a rack-mounted unit.

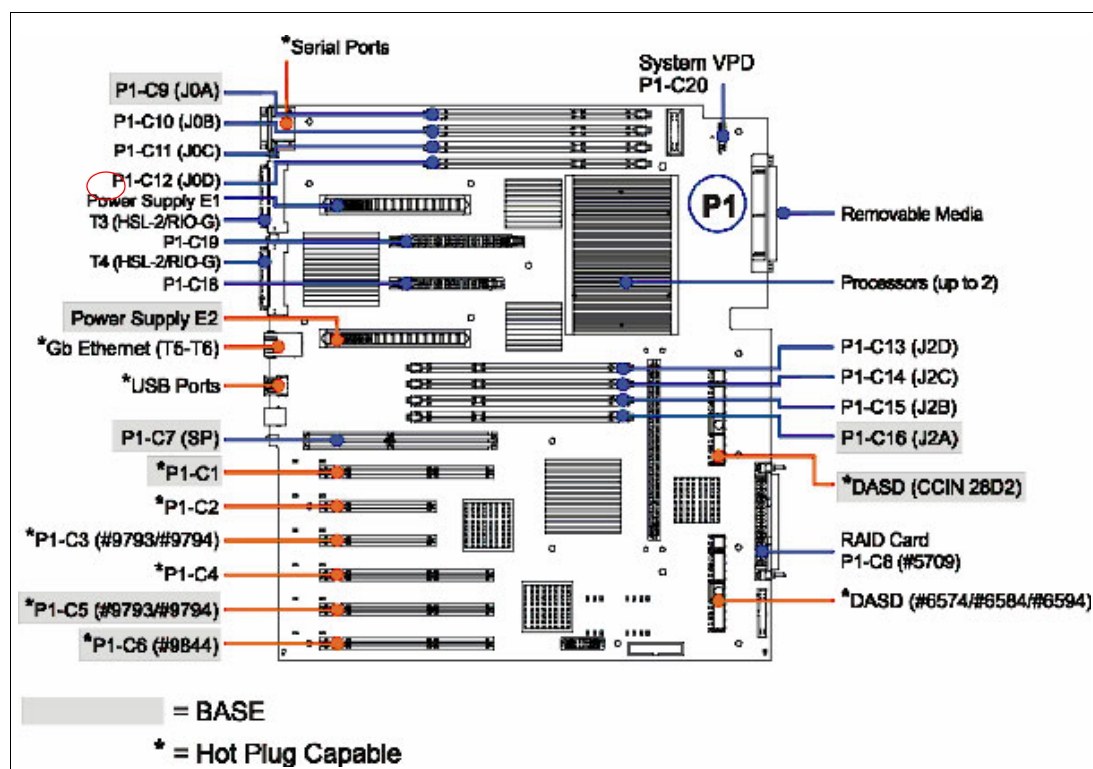


Figure 1-5 i520 plan view

Figure 1-6 shows the rear of the i520/550. You can see the connections for the HMC, the high-speed link (HSL), the system power control network (SPCN), local area network (LAN), and the service ports. There are also Universal Serial Bus (USB) ports. These are not usable by i5/OS. Both of the Ethernet ports are available for allocation to partitions, but cannot be used for Operation Console LAN connection. SPCN is a loop on i5 servers. Therefore, both of the ports will have a cable connected if an expansion tower is a part of the system.

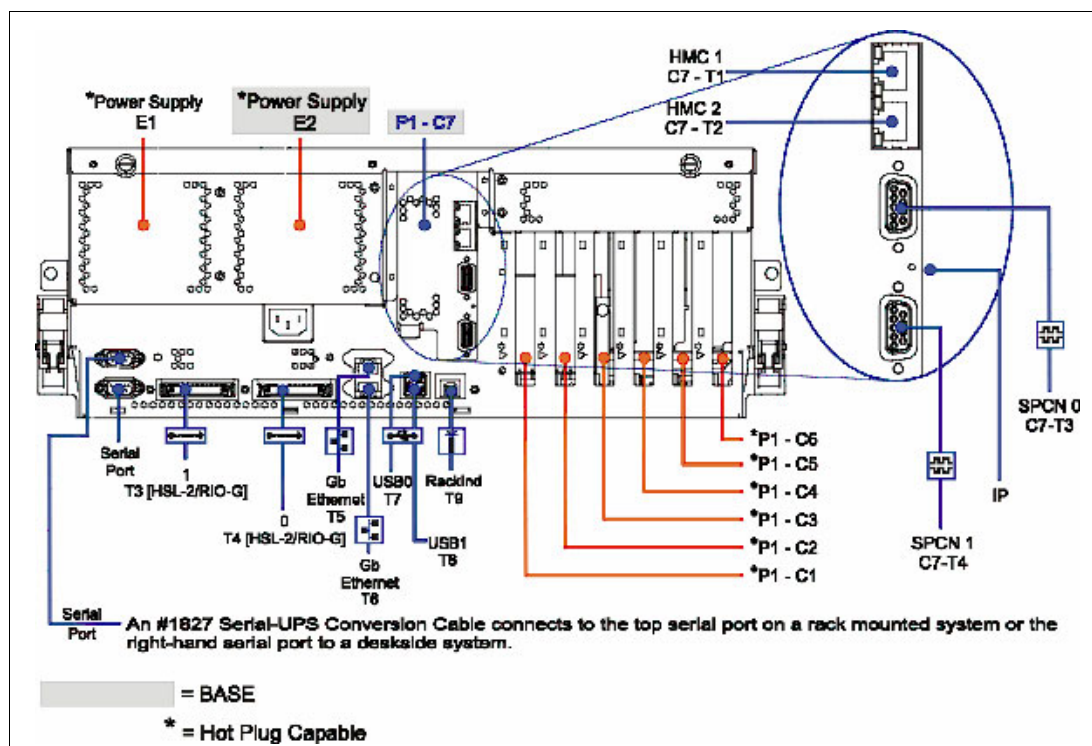


Figure 1-6 i520 rear view

The front view presents you with a standard SCSI bay for an internal tape drive. There are two integrated development environment (IDE) drive bays for a DVD device. The lower bay is IDE, but it has a SCSI converter to allow connections to the i5/OS. The second or upper bay can have a DVD device that is IDE-connected.

In the control panel, there is a USB and an Ethernet port. Neither of these items is available for use by the partitions. The controls for accessing the display messages and entering the options are very similar to the current 8xx operation panel.

There are eight disk drive bays, arranged in two groups of four. With the #5709 feature, the bays P3D1 - P3D4 can run with no protection or mirroring. The #5709 feature is located behind the drill panel beneath the disk bays. This adapter can have a #6574 feature added as a daughter card. This enables these four disks to run RAID protection.

To include the other four disk bays, a #6594 feature must be added. This provides the disk bay back plane for bays P2D1 - P2D4. The protection for these disks can be RAID or mirroring. P3D1 is the first disk slot for an i5/OS load source device. The configurator forces you to put a disk in the load source position, but in a partitioned server, there is no requirement for a load source disk in the CEC.



If you want to run these disks under a separate partition, they must be driven by an IOP/IOA from one of the PCI-X slots in the CEC (Figure 1-7).

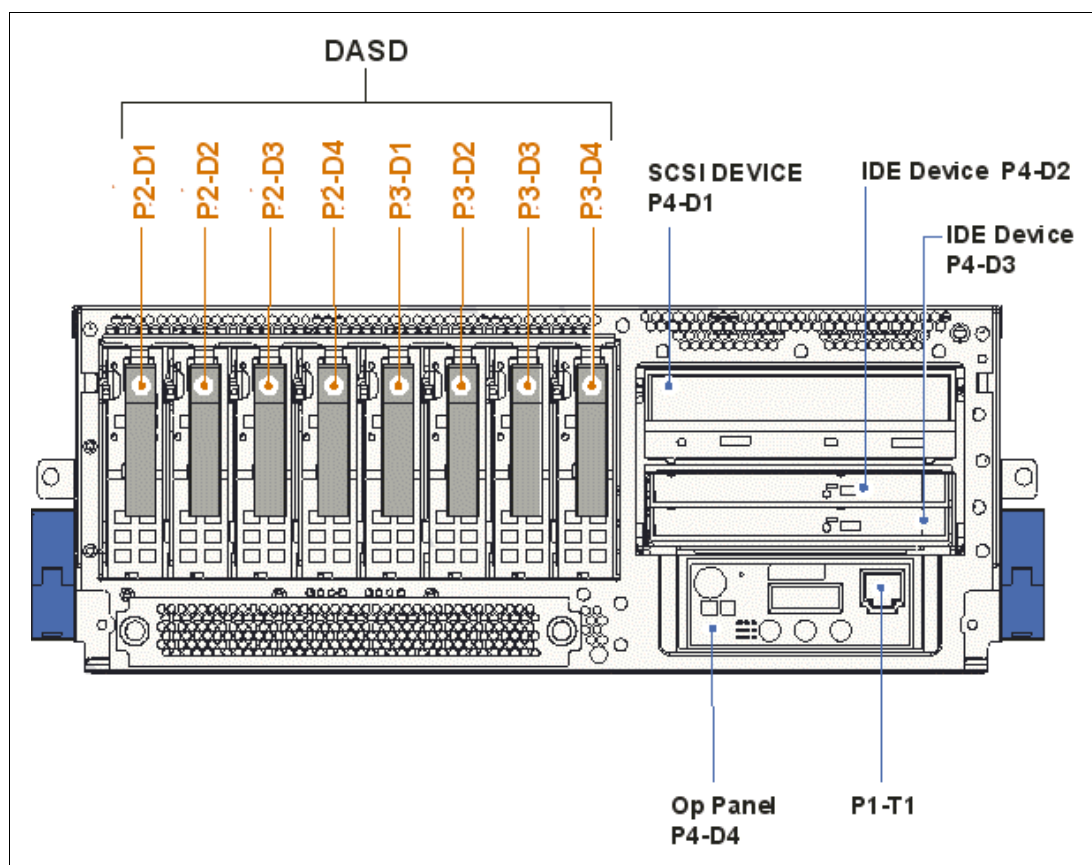


Figure 1-7 i520 front view

Table 1-3 shows the physical specifications for model 520.

Table 1-3 Model 520 physical specifications

Model 520	Width	Depth	Height	Weight
Rack-mounted drawer	437 mm (17.2 in)	508 mm (23 in)	178 mm (7 in)	43 kg (95 lb)
Stand-alone server	201 mm (7.9 in)	584 mm (23 in)	533 mm (21 in)	43 kg (95 lb)
#0588 / #5088	485 mm (19.1 in)	1075 mm (42.3 in)	200 mm (8.0 in)	68 kg (150 lb)
#0595	432 mm (17 in)	686 mm (27 in)	178 mm (7 in)	42.7 kg (94 lb)
#5094	485 mm (19.1 in)	1075 mm (42.3 in)	910 mm (35.8 in)	280 kg (617 lb)
#5095	246 mm (14.5 in)	800 mm (31.5 in)	556 mm (21.9 in)	52.7 kg (116 lb)
#5294	216 mm (8.5 in)	1020 mm (40.1 in)	1800 mm (71 in)	726 kg (1600 lb)



Table 1-4 shows details about the operating environment.

*Table 1-4 Model 520 operating environment*

Operational component	Operational value
kVA (maximum)	0.789
Rated voltage and frequency	100-127 / 200-240 AC @ 50/60 Hz (+/- 0.5)
Power consumption	750 watts
Thermal output	2557 BTU/hr
Noise level	<ul style="list-style-type: none"><li>▶ Rack drawer: 6.0 bels</li><li>▶ Stand-alone: 6.8 bels</li></ul>
Inrush and leakage current	85 / 1.15
Temperature	5 - 35 degrees C (41 - 95 degrees F)
Noncondensing humidity	8% - 80%
Wet bulb temperature	23 degrees C (73.4 degrees F) (operating)

## The i570 physical layout

Figure 1-8 shows the plan view of model i570. This model is rack-mount only and uses blindswap cassette technology so that you will not get to see the inside of this server.

The I/O adapters can all be removed from the rear of the server. Other components can be accessed through the front of the server.

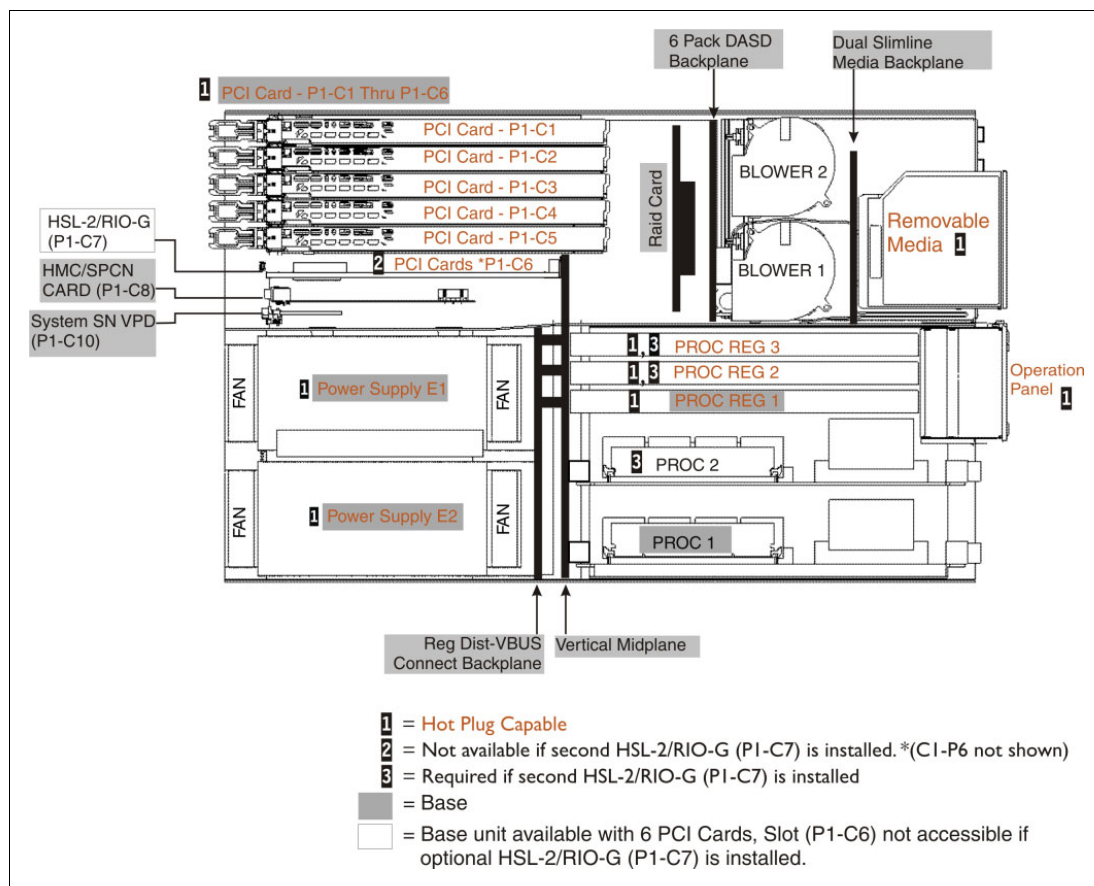


Figure 1-8 i570 plan view

The rear of the i570 (Figure 1-9 on page 21) has the blindswap cassettes on the left and power supplies to the right. Between the I/O adapters and the power supply is the Service Processor.

There are two types of blindswap cassettes, one for card slot 1 - 5, and a different type for slot 6. (The cassette for slot 6 is different because it can accommodate the second HSL-2 adapter.)

On the lower right is the system interconnect port. This allows multiple i570s to be connected to form a large operating unit.

As with the i520, there are LAN, SPCN, HSL, and USB ports. (The USB ports are not available for use by the i5/OS. The LAN ports are available for partition use, but they are not available for Operations Console LAN.)

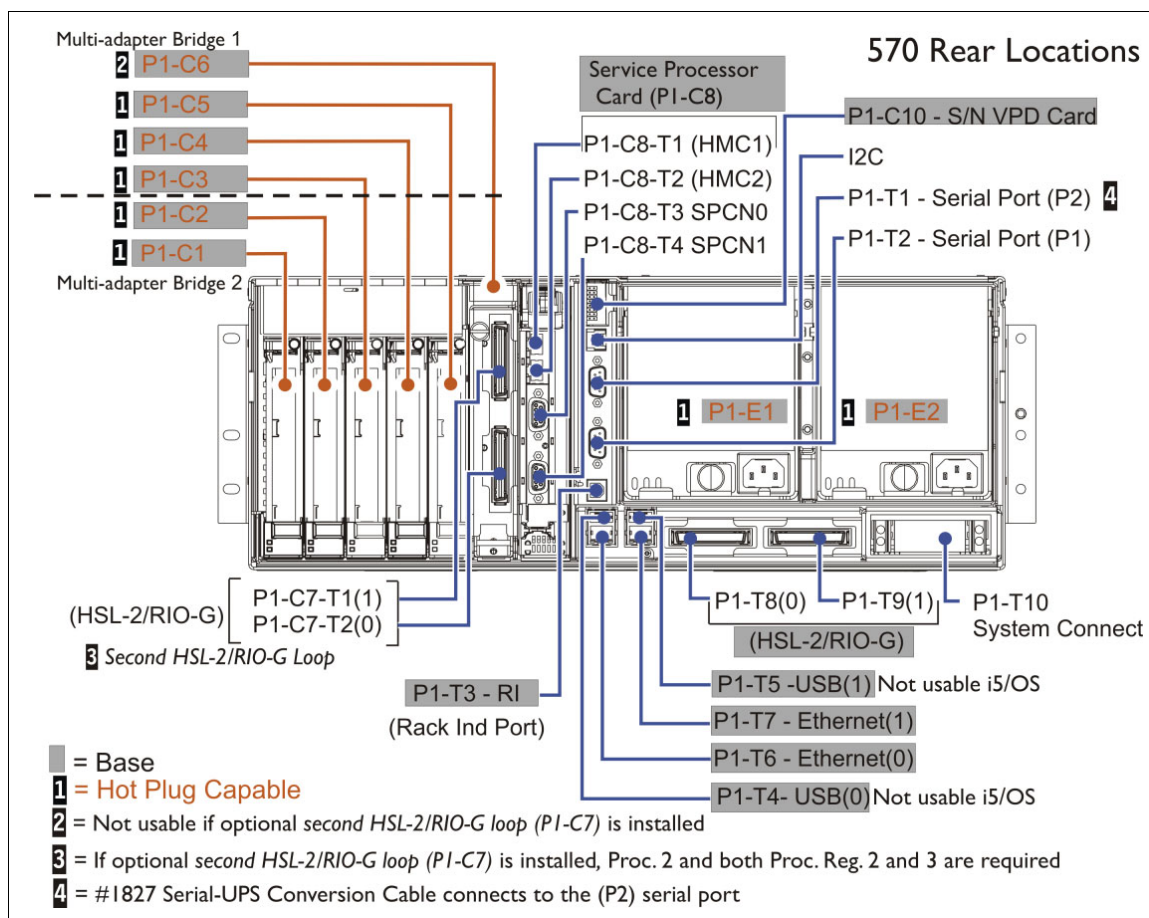


Figure 1-9 i570 rear view

If you look at the front of the i570, you see two DVD device drive bays. However, there is no bay for an internal tape drive. If a tape is required, it must be internal, in an expansion tower, or an external drive. As with the i520, only one of the DVD drive bays is available for i5/OS use.

In the control panel, there are USB and Ethernet ports. Neither of these is available for use by the partitions. The controls for accessing the display messages and entering the options is very similar to the current 8xx operation panel.

There are six disk bays in the i570.

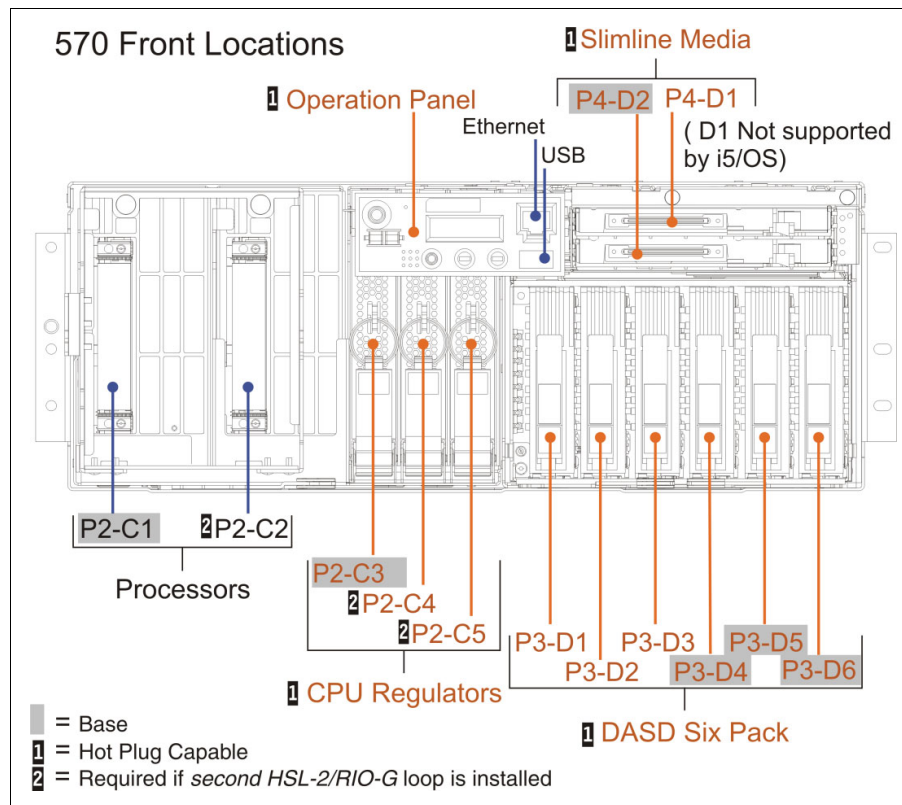


Figure 1-10 i570 front view

Table 1-5 describes the physical features of the i570.

Table 1-5 Model 570 physical specifications

Model 570	Width	Depth	Height	Weight
System unit	483 mm (19 in)	790 mm (31.1 in)	174.1 mm (6.85 in)	63.6 kg (140 lb)
#0588 / #5088	485 mm (19.1 in)	1075 mm (42.3 in)	200 mm (8.0 in)	68 kg (150 lb)
#0595	432 mm (17 in)	686 mm (27 in)	178 mm (7 in)	42.7 kg (94 lb)
#5094	485 mm (19.1 in)	1075 mm (42.3 in)	910 mm (35.8 in)	280 kg (617 lb)
#5095	246 mm (14.5 in)	800 mm (31.5 in)	556 mm (21.9 in)	52.7 kg (116 lb)
#5294	216 mm (8.5 in)	1020 mm (40.1 in)	1800 mm (71 in)	726 kg (1600 lb)

Table 1-6 shows the operating environments for model 570.

*Table 1-6 Model 570 operating environment*

kVA (maximum)	1.474
Rated voltage and frequency	100-127 / 200-240 AC @ 50/60 Hz (+/- 0.5)
Power consumption	1400 watts
Thermal output	4774 BTU/hr
Noise level	<ul style="list-style-type: none"><li>▶ Rack drawer: 6.0 bels</li><li>▶ Stand-alone: 6.8 bels</li></ul>
Inrush and leakage current	85 A / 3m A
Temperature	5 - 35 degrees C (41 to 95 degrees F)
Noncondensing humidity	8% - 80%
Wet bulb temperature	23 degrees C (73.4 degrees F) (operating)

## 1.5 Linux migration

This section provides a brief overview of the Linux migration process. For more information about the migration of an existing Linux partition on an iSeries system to a System i5, refer to the following Web site:

<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/iphbi/iphbimigratiseries.htm>

Upgrade planning for Linux partitions is a relatively new concept because the guest partition has not been available for very long. Consider the following three upgrade possibilities:

- ▶ Upgrading their Linux version to a new release.
- ▶ The effect of hardware upgrades on their Linux partitions.
- ▶ A new Linux kernel is required to run on System i5 hardware.

When upgrading to a new version of Linux, understand whether the distributor supplies an upgrade mechanism. When you upgrade from V5R1 to V5R3 or later, you must upgrade your Linux OS from 32-bit to 64-bit. You must also review your distributor's support for IBM PowerPC® 64-bit.

The second consideration is the hardware support for Linux partitions and the native adapter support. If you have any IOAs that you are planning to change as you upgrade, move these from the virtual disk to the native-attached SCSI disk or the fibre channel disk. You must also provide or change the installed disk driver in your Linux partition.

Upgrading with Linux partitions built over virtual devices is the simplest environment, provided the OS environments are upgraded. You can vary off the Linux server and vary it back on after the upgrade, assuming that none of the resource naming is changed.

### 1.5.1 Migrating a Linux logical partition from iSeries

Migrate a Linux logical partition from iSeries as follows:

1. In your existing server, upgrade to a version of Linux that supports the System i5 servers. Contact the Linux distributor for detailed instructions.
2. In your existing server, replace the existing I/O device drivers with the iSeries virtual I/O device drivers.
3. From the new Linux distribution, retrieve the Linux kernel that supports the System i5 POWER5 processors and store it in the OS/400 file system.

## 1.6 Windows migration

This section provides a brief overview of the Windows server migration process.

Moving the Windows server installations to new hardware is much simpler in an Integrated xSeries Server (IXS) or Integrated xSeries Adapter (IXA) environment than in an external stand-alone server environment. This section briefly outlines the upgrade process when the IXA or IXS card is physically moving to the new hardware. Other scenarios are explained in the Windows migration chapter.

An IXS card located in 8xx CEC slots must be accommodated in an expansion when upgrading to a System i5 because they cannot be accommodated in any of the 5xx CEC slots.

### 1.6.1 Moving the Integrated xSeries Adapter or Integrated xSeries Server from iSeries 8xx to 5xx

Perform the following tasks to move the IXS and the IXA from iSeries 8xx to 5xx:

1. Ensure that the iSeries server is at V5R3 or later.
2. Install the latest program temporary fixes (PTFs) on iSeries.
3. Upgrade the integration software on the xSeries:
  - a. Select **Start** → **Programs** → **IBM iSeries** → **Integration for Windows Server**.™
  - b. Select the server you want to upgrade.
  - c. Right-click and select **All tasks** → **Update**.
4. Back up your xSeries server.
5. During the upgrade to the iSeries hardware, move the IXA or IXS card to its new position in the new iSeries server.
6. Change the resource name in the nonprogrammable workstation (NWS) description.
7. Vary on and use as normal.

## 1.7 IBM AIX 5L migration

Because AIX 5L™ is not supported on iSeries 8xx servers, this is not a migration issue. Any required AIX partitions can be set up and the data migrated subsequent to the model upgrade.

**Note:** Historically, model upgrades have not been offered in the AIX marketplace. Therefore, this scenario is not unusual for the AIX client base.

For more information about AIX 5L implementation, refer to *AIX 5L on IBM System i Platform Implementation Guide*, SG24-6455.

For information about upgrades to the system within the System i5 range, consult the AIX 5L upgrade pages at:

<http://www.ibm.com/servers/aix/upgrade/index.html>

## 1.8 Migration and upgrade check list

Table 1-7 contains a checklist that you can print to prepare for your upgrade and migration plan. During your planning process, customize this checklist and use it as a structure to help you identify what you must do for your particular situation and availability requirements.

Table 1-7 Migration and upgrade planning checklist

Task	Brief description	Due date / task owner	Where to find additional information
<b>General planning task</b>			
____ Task	If you have not already done so, make a copy of this checklist and put it in your project book.	____/____/____ _____	
____ Task	Organize your project book and project documents.	____/____/____ _____	
____ Task	Perform physical planning tasks to make sure that you have adequate space and power for your upgraded system. Be sure to consider the differences in cabling requirements.	____/____/____ _____	Visit the physical site planning site, which is available on the Web at: <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp">http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp</a>
____ Task	Verify your planned configuration.	____/____/____ _____	
____ Task	If you have not already done so, determine whether you have to order replacements for unsupported hardware devices.	____/____/____ _____	
____ Task	If your system exchanges information with other AS/400s or iSeries, plan any required changes to ensure the coexistence of different OS releases.	____/____/____ _____	
____ Task	If you have not already done so, determine whether you will use IBM services for any part of the upgrade process.	____/____/____ _____	

Task	Brief description	Due date / task owner	Where to find additional information
____ Task	Have the software and the publications been ordered on CD-ROM?	____/____/____ _____	Validate with your local IBM Software Order organization.
____ Task	Has the user-based pricing been specified with the correct number of users?	____/____/____ _____	Validate with your local IBM Software Order organization.
<b>Hardware configuration tasks</b>			
____ Task	Was an IBM-supplied configurator tool used for hardware and software configuration?	____/____/____ _____	
____ Task	If LPARs are going to be used, was the LVT used?	____/____/____ _____	
____ Task	Will Linux or AIX partitions be installed?	____/____/____ _____	
____ Task	<ul style="list-style-type: none"> <li>▶ With Linux or AIX, will direct I/O or virtual I/O be used?</li> <li>▶ What tape will be used for the Linux/ AIX partition backup?</li> </ul>	____/____/____ _____	
____ Task	Does the configured system meet or exceed any capacity planning tool recommendations?	____/____/____ _____	
____ Task	Are the number of DASD arms and DASD IOAs sufficient for the client's planned DASD protection?	____/____/____ _____	
____ Task	Has the appropriate feature code for mirroring or RAID protection been ordered?	____/____/____ _____ -	
____ Task:	Will the quantity and speed of the tape devices be able to meet the client's backup window requirements?	____/____/____ _____	
____ Task	Will all the products be delivered by the planned installation date?	____/____/____ _____	
____ Task	Is there an established timetable for software and hardware setup and installation?	____/____/____ _____	
____ Task	Has the appropriate amount of main storage memory been ordered?	____/____/____ _____	



Task	Brief description	Due date / task owner	Where to find additional information
____ Task	Does the hardware support the client's availability plan (DASD, Tape, LAN, and Communication lines)?	____/____/____ _____	
____ Task	If non-IBM hardware will be attached to the system (especially non-IBM DASD), has the client verified whether it is supported?	____/____/____ _____	Check with third-party product suppliers.
____ Task	Does the source system include migration or SPD towers?	____/____/____ _____	
____ Task	Will the currently installed tower be converted to HSL/PCI towers?	____/____/____ _____	
____ Task	If no migration tower is going to be used, have PCI replacement features been ordered to replace the installed SPD features?	____/____/____ _____	
____ Task	Is space required for a load source pump?	____/____/____ _____	
____ Task	If the load source is going to be protected with RAID, has the proper amount of additional disk been ordered (3/7/9) for the RAID set required?	____/____/____ _____	
____ Task	Has the appropriate console type been configured (twinaxial, operations navigator, or HMC)?	____/____/____ _____	
____ Task	Has an appropriate device been ordered or is it already available for the console type?	____/____/____ _____	
____ Task	If 10k rpm disks are to be migrated to HSL towers, is there room to accommodate them?	____/____/____ _____	
____ Task	Has the method to migrate data from nonconverted disk been identified?	____/____/____ _____	
<b>Installation plan tasks</b>			
____ Task	Has a site preparation review been planned?	____/____/____ _____	
____ Task	Has the removal of migrated/replaced equipment been planned?	____/____/____ _____	

Task	Brief description	Due date / task owner	Where to find additional information
____ Task	Does the client understand which parts of this installation are the client's responsibility and which are the IBM Service Representative's responsibility?	____/____/____ _____	
____ Task	Have the appropriate installation manuals for both hardware and software been ordered for the client on CD-ROM?	____/____/____ _____	
____ Task	Does the client agree with the installation plan?	____/____/____ _____	
____ Task	Has the client committed personnel and resources to the project?	____/____/____ _____	
____ Task	Will the client location be able to move the system to the installation site from the delivery dock? Is the height, width, depth, and load capacity of any elevator to be used adequate for system?	____/____/____ _____	See the physical planning site: <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp">http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp</a>
____ Task	Have the names of the movers and the installation group been given to the client's security personnel?	____/____/____ _____	
____ Task	Will additional/special tools be required to move the equipment to the client's machine room?	____/____/____ _____	
<b>Software checklist</b>			
____ Task	Has the required level of OS/400 been ordered?	____/____/____ _____	
____ Task	If LPARs are going to exist, will they have valid OS/400 releases for the hardware and the primary partition?	____/____/____ _____	
____ Task	Will the installed system be upgraded to the required level of OS/400 before the upgrade, and if so, when?	____/____/____ _____	
____ Task	Are the current cumulative program temporary fix (CUM PTF) packages available?	____/____/____ _____	
____ Task	Has the Preventive Service Planning (PSP) package been reviewed and understood?	____/____/____ _____	

Task	Brief description	Due date / task owner	Where to find additional information
____ Task	Has the HIPER PTF list been reviewed and the PTF ordered?	____/____/____ _____	
____ Task	Are there any unsupported software/licensed program product (LPP)/programming request for price quotation (PRPQ) that have to be replaced or altered? Are alternatives known, and have they been ordered (for example, OV/400, client access, or fax)?	____/____/____ _____	
____ Task	Has the memo to user section titled "Licensed products that are no longer supported" been reviewed?	____/____/____ _____	
____ Task	Check the current installed client software for compatibility, that is, iSeries access.	____/____/____ _____	
____ Task	Plan to upgrade the client software to the latest release and service pack.	____/____/____ _____	
____ Task	If the upgrade is a side-by-side where all the client applications, libraries, and data will be restored to a new system, have alternative provisions been made to capture information contained in OUTQ, DTAQ, and MSGQ, if necessary?	____/____/____ _____	
<b>Site preparation tasks</b>			
____ Task	Is the site preparation on schedule?	____/____/____ _____	
____ Task	Has proper power installation been ordered for all the systems, the new I/O towers, and the additional equipment required during the upgrade only or any external equipment?	____/____/____ _____	
____ Task	Are the power connectors correct for the new system unit and the I/O tower?	____/____/____ _____	Refer to the iSeries physical planning Web site at: <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp">http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp</a>

Task	Brief description	Due date / task owner	Where to find additional information
____ Task	If using side-by-side, is power available to run both the systems at the same time?	____/____/____ _____	
____ Task	Have all the preparations for cooling and grounding been met?	____/____/____ _____	
____ Task	Has the client considered contracting an IBM Installation Planning Representative?	____/____/____ _____	
____ Task	Have all the physical planning check lists from the physical planning Web site been completed?	____/____/____ _____	Refer to the iSeries physical planning Web site at: <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp">http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp</a>
____ Task	Does the client understand that it is their responsibility to order, install, and assemble all the twinaxial, coax, telephone twisted pair, Ethernet, and IBM cabling system cables?	____/____/____ _____	
____ Task	Have all the cables and connectors been ordered and confirmed?	____/____/____ _____	Refer to the iSeries physical planning Web site at: <a href="http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp">http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp</a>
____ Task	Has the floor plan layout been completed?	____/____/____ _____	
____ Task	Is there adequate storage space for manuals, tools, and cleaning kits?	____/____/____ _____	
____ Task	Is the client aware that a relatively short power outage can cause a significantly long system outage? Has a UPS been installed or ordered? Has the physical planning and capacity planning for the UPS been done?	____/____/____ _____	
<b>System management tasks</b>			
____ Task	Have the system components been labeled?	____/____/____ _____	
____ Task	Have adequate training and update sessions been scheduled?	____/____/____ _____	

Task	Brief description	Due date / task owner	Where to find additional information
____ Task	Has training for the HMC been scheduled?	____/____/____ _____	
____ Task	Will programmers be trained to take advantage of the new functions and the OS/400 unique features and functions?	____/____/____ _____	
____ Task	Has a standard for the application's documentation been established?	____/____/____ _____	
____ Task	Has a standard for the operations been documented in a particular HMC?	____/____/____ _____	
____ Task	Are plans in place for ongoing management of disk space usage?	____/____/____ _____	
____ Task	Are there defined change management procedures in place?	____/____/____ _____	
____ Task	Are non-IBM software impacts known and documented?	____/____/____ _____	
____ Task	Are schedules in place for preventive maintenance for both hardware and software?	____/____/____ _____	
____ Task	Does the client understand the use of electronic customer support (ECS), Web-based support, and other IBM-supplied problem determination tools?	____/____/____ _____	
____ Task	Is the save/restore strategy adequate for the new system?	____/____/____ _____	
____ Task	Are the quantity and speed of tape devices adequate for the client to complete daily backups within the required window?	____/____/____ _____	
____ Task	Have the networking options been reviewed?	____/____/____ _____	
____ Task	Has the communication network been checked to ensure compatibility across all the products in the network?	____/____/____ _____	

Task	Brief description	Due date / task owner	Where to find additional information
____ Task	Has IBM Technology Services been offered to assist in the installation of all or part of the hardware, software, or configuration of the network/communication?	____/____/____ _____	
____ Task	If planning for a TCP/IP network, has a unique Internet domain name been registered?	____/____/____ _____	
____ Task	If the client is planning to connect to the Internet, are appropriate security measures planned or implemented?	____/____/____ _____	
<b>Testing. tasks</b>			
____ Task	Plan how to validate your applications.	____/____/____ _____	
____ Task	Plan how to check network communications and client software.	____/____/____ _____	
<b>The following table is for user defined tasks:</b>			
____ Task		____/____/____ _____	
____ Task		____/____/____ _____	
____ Task		____/____/____ _____	
____ Task		____/____/____ _____	
____ Task		____/____/____ _____	
____ Task		____/____/____ _____	
____ Task		____/____/____ _____	



## Migration examples

This chapter provides some examples of a general upgrade and migration process and certain advanced situations. Before reading this chapter, you must have an understanding of the planning considerations and migration options described in Chapter 1, “Planning for upgrades to System i5 hardware” on page 1.

**Important:** The steps and descriptions in this chapter are for guidance only. Steps, processes, and responsibilities might change. If you are planning an upgrade using a supported miscellaneous equipment specification (MES), the Customized Upgrade Installation Instructions (CUII) will always be the correct document to describe the upgrade. For an unsupported migration using an upgrade method, you should seek advice from your IBM Representative before attempting the upgrade.

## 2.1 General upgrade considerations

When you plan your specific upgrade, certain model-related considerations must be taken into account because these affect your decision pertaining to the upgrade method chosen.

Following are the supported model upgrades to new models:

- ▶ 810 or 820 to 520, 550
- ▶ 820, 825, 830, 840, 870, and 890 to 570, 595

This section also discusses data migration from models that do not support V5R3 or later.

Following are the five methods you can use to upgrade to the new models:

- ▶ Upgrade using the side-by-side method
- ▶ Data migration using the side-by-side method (source system at previous release)
- ▶ Upgrade using the unload/reload method
- ▶ Upgrade with converted or relocated disks
- ▶ Upgrade with load source migration

These methods apply to both logical partitioned systems and nonlogical partitioned systems.

If you are upgrading a logical partitioned server, additional considerations must be kept in mind. In the new hardware, there is no P0 primary partition. The functions of the primary partition are taken over by the flexible service processor. When upgrading, the logical partition (LPAR) migration tool allocates partition numbers, maintaining, where possible, the current numbering scheme. P0 becomes the next available number, for example, a server with partitions P0, P1, P2, and P3 will migrate to a server with partitions P1, P2, P3, and P4, where P1...P3 are as before, and P4 is the old P0.

**Note:** When we refer to the side-by-side or unload/reload methods here, we are discussing the style of upgrade or migration. This does not necessarily mean that the marketing features for a side-by-side or unload/reload have been configured on e-Config.

Table 2-1 compares the upgrade methods. The option with the least risk is a combination of side-by-side (to test) and relocated disks (for the final upgrade), when possible.

Table 2-1 Comparison of upgrade methods

Method	Complexity	Time to upgrade	Risk
Side-by-side	High	Medium	Low
Data migration	High	Medium	Low
Unload/Reload	High	High	High
Relocated disks	Low	Low	Medium
Load source migration	Medium	Medium	Medium



## 2.1.1 Side-by-side upgrade and data migration using the side-by-side method

The side-by-side upgrade path is a method where the target system is a complete (or near-complete) replacement for the source system. This is of two types:

- ▶ Side-by-side, retaining the existing serial number (that is, a side-by-side upgrade).
- ▶ Side-by-side with a new serial number, that is, a box swap and not an upgrade. This is used often when there is no supported upgrade path from the client's existing system, as a data migration to a new system. If the source system is a model that does not support the V5R3 or later level of OS/400, there are additional steps in the upgrade path.

Both the methods involve the purchase of enough resources to duplicate most or all of the current environment.

### Side-by-side upgrade

In the side-by-side upgrade method, with IBM approval, an IBM service contract, or both there may be limited use of the MES hardware for a short time to carry out extended user testing, thereby reducing the total upgrade risk and possibly reducing the downtime. The benefit of this method is that the production machine is unavailable only during the normal backup routines.

The source system supports V5R3 or later. This method is used to test the upgrade process and gives the users the time to test the new environment.

This is the sequence of events in the upgrade process:

1. The client reviews the information Request for Price Quotation (RPQ) and orders upgrade, services, and side-by-side time through a special bid process.
2. The required hardware is ordered to duplicate most or all of the environment.
3. The source system is upgraded to V5R3 or later in all the partitions.

**Note:** If you are upgrading the source system to i5/OS V5R4, a 17 GB load source is required for any i5/OS V5R4 partition.

4. The MES is installed as a stand-alone system.
5. The LPAR configuration is created on the target server.
6. Existing full system backups are used to create the new test system using the recovery procedures described in *Backup and Recovery V5R4*, SC41-5304-08, which is available at:  
<http://www.elink.ibm.link.ibm.com/publications/servlet/pbi.wss?SSN=07AHN0027542911678&FNC=PBL&PBL=SC41-5304-08PBCEEB0200012125&TRL=TXTSRH>
7. The client tests the current environment for up to 56 days.
8. Any production objects that are created or altered, and which will be required on a new system, are saved.
9. The target server is then synchronized with the source system. This can be done in a number of ways:
  - Install only changed objects (saved with the save changed objects command).
  - Install client data libraries only (assuming that the program libraries are unchanged).
  - Scratch install from up-to-date source system saves.

- Follow the disk migration upgrade path outlined in 2.1.4, “Upgrade with converted or relocated disks” on page 38.

**Important:** Although scratch install is the safest way to ensure that all of the objects are synchronized, it might take an excessive amount of time. The method allows for an intermediate stage where the target system is refreshed with the changed data to test the final upgrade method.

When using the save changed objects command, the client must be sure that the testing process does not change the data objects. Otherwise, data mismatches occur.

Refer to *Backup and Recovery V5R4*, SC41-5304 for detailed procedures.

10. Move any required hardware from the source to the target system.
11. Perform full system backups.
12. Go live.

## 2.1.2 Data migration using the side-by-side method (source system in the previous release)

In the data migration side-by-side upgrade method, a new server is installed with a serial number that is different from the existing server's because no upgrade path exists to the new hardware. The benefit of this method is that the production machine is unavailable only during normal backup routines.

You might chose to use this method:

- ▶ When the source system does not support the V5R3 or later release of OS/400.
- ▶ When the source system will not support a 17 GB load source drive.

The tasks involved in the upgrade process are:

1. The client orders a new server and services through a special bid process.
2. The new system duplicates most or all of the current environment.
3. The source system is upgraded to the highest release it can support.
4. The new server is installed.
5. If the new server has licensed programs installed, scratch install the System Licensed Internal Code (SLIC) and the base OS/400.

**Note:** A new system might be delivered with V5R3 and the licensed programs installed. In order to ensure a complete system migration, the target system must be scratch installed with only the V5R3 Licensed Internal Code and the base operating system.

For more details, refer to “Restoring Previous Release User Data to a New System” in *Backup and Recovery V5R4*, SC41-5304-08.

6. Existing full system backups are used to create the new test system, using the recovery procedures described in *Backup and Recovery V5R4*, SC41-5304-08.
7. Upgrade the licensed programs to i5/OS V5R3 or later.
8. Install the latest PTFs.

9. The client tests the current environment.
10. Any production objects that are created or altered, which will be required on the new system, are saved.
11. The target server is then synchronized with the source system. This can be done in a number of ways:
  - Install only the changed objects (saved with the save changed objects command).
  - Install only the client data libraries.
  - Scratch install from the up-to-date source system saves.

**Important:** Although scratch install is the safest way to ensure that all the objects are synchronized, it might take an excessive amount of time. This method allows for an intermediate stage where the target system is refreshed with the changed data to test the final upgrade method.

When using the save changed objects command, the client must be sure that the testing process does not change data objects. Otherwise, data mismatches can occur.

Refer to *Backup and Recovery V5R4*, SC41-5304-08 for information about the detailed procedures.

12. Move the required hardware, if any, from the source to the target system.
13. Perform full system backups (you require system saves in i5/OS V5R4 for recovery).
14. Go live.

### 2.1.3 Upgrade using unload/reload

This is a dramatic upgrade where the entire system is saved to tape and restored on the new system. This method is used when large amounts of hardware are moved from the source system to the target system, and the target system, as delivered, does not have sufficient hardware to perform a side-by-side. This method is the least desirable option.

If the target system has sufficient hardware to be used as a system, a side-by-side is recommended to minimize the risks. Failback is possible in the event of failure.

The unload/reload scenario follows the same process as that described previously except that a new system is built with vital components (disk and I/O adapters) from the existing system. Thus, for a short time, when the customer engineer (CE) is performing the hardware upgrade, the client's data is only on tape; that is, the source system has the vital components removed, leaving it a lifeless hulk, and the target system is not yet built. Failback can involve a scratch install back onto the old hardware. However, this is time-consuming and will possibly take too long for the business to stand.

This is the process:

1. The vital system components move from the source to the target system. Other migration methods cannot be used.
2. Ensure a common tape media between the systems.
3. Upgrade all the partitions to i5/OS V5R3 or later release, with the latest cumulative pack, HIPER, and hardware related PTFs.
4. Perform a full system backup (at least two copies to guard against media error).
5. Check the job log to ensure that the saves are completed successfully.

**Important:** Be absolutely certain that the saves are completed successfully because data that is not saved cannot be recovered by using this method.

6. Remove the hardware from the source system and perform an MES upgrade.
7. Scratch install a new system from the saves.
8. Perform resource mapping.
9. Perform a test and go live.

#### 2.1.4 Upgrade with converted or relocated disks

This method is the standard 8xx to 5xx upgrade and offers a plug-and-go upgrade. If it is well-planned, it can be the fastest form of upgrade. If many disks are being moved, there is always the risk of inadvertent damage, for example, a bent pin or a disk not starting. Although these can cause major problems, they are rare occurrences.

This is the simplest process of upgrading, provided there are no SPD-attached devices. Assuming there are no SPDs, this is the outline of this process:

1. Bring the current server and any partitions up to i5/OS V5R4 with the latest PTFs.
2. Ensure that there is space in the new system for the disk to be removed and relocated from the existing system unit.
3. Make sure that there is space for the I/O adapters to be relocated to the new server.
4. Perform a full system backup.
5. Power down the existing server.
6. Remove the disks and the I/O adapters.
7. Plug the disks into the new system unit.
8. Install the I/O adapters in the new system.
9. Upgrade or migrate any towers that are moving across.
10. Cable up the System Power Control Network (SPCN) loop.
11. Cable the high-speed link (HSL) (care must be taken to maintain bus numbering if there is an LPAR).
12. Run the LPAR migration program.
13. Power up.
14. Fix any ownership and resource naming issues.
15. Add the new resources to the system.
16. Go live.

Consider these points:

- Model 820 to model 520/550 upgrade. The 820 has six disk bays and the 520/550 has four disk bays in the base configuration. If this is not noticed, circumstances where there are too many disks from the system unit to fit into the new system unit may arise. The configurator will place the “overspill” hardware in another expansion unit.

This might result in the existing Redundant Array of Independent Disks (RAID) set being broken, which causes the upgrade to fail. The client will have to remove the “overspill” disks from the existing RAID set before the upgrade. An additional consideration in this

scenario is that the “overspill” disk might force an unwanted expansion unit and significantly increase the MES price.

- ▶ Bus cabling must be planned to ensure that buses retain their existing numbering wherever possible.
- ▶ SPCN is cabled as a loop in the new hardware.

### 2.1.5 Upgrade with load source migration

This upgrade is primarily used to upgrade from a 7xx model to a new 5xx. Because this is an unsupported upgrade path, additional services must be purchased to perform this upgrade. This can be used for both logical partitioned servers and nonlogical partitioned servers. This upgrade maintains the client investment in the disk and provides an easy transition to the new server.

This upgrade involves the following steps:

1. Upgrade the current system to V5R3 or later with the latest PTFs.
2. The order must include PCI versions of all the required SPD hardware.
3. Migrate all the data from the system unit to the disks in the 5065/5066 tower.
4. Perform a full system backup.
5. Load the source migration to the 5065/5066 tower.
6. Relocate any disks that must be repackaged in the new PCI expansion towers. Care must be taken to retain the exact position and RAID arrangement.
7. Convert the 5065/66 expansion towers to Peripheral Component Interconnect high-speed link (PCI/HSL).
8. Remove all of the SPD hardware.
9. Connect all of the converted hardware and the new hardware.
10. Run the LPAR migration tool.
11. Check the resource allocation, particularly the load source for the partition that was P0.
12. Perform a full system backup.
13. Test and go live.

If you employ this method for an 8xx to 5xx upgrade, you can use any 5065 or 5066 that is being upgraded to move the load source (load source on model 5xx does not have to be in the system unit). Here, you must use disk migrate when active in order to move all the data from the disks in the system unit and remove them from the configuration. The final task is to copy the load source unit to the tower.

During the upgrade, you can simply relocate any PCI I/O adapters in the system unit to the new locations in the new system unit. Run the LPAR migration tool and then fix the ownership issues, if any, and resource naming and allocation of new resources.

Consider the following points:

- ▶ Is it cost-effective to keep older drives?
- ▶ How will you maintain RAID sets during Disk Migrate While Active (DMWA) or physical relocation?
- ▶ What is the impact of changing two buses to three when upgrading 5065/5066?

## 2.2 Migration examples

This section provides a few examples of physical migration or upgrade.

### 2.2.1 Model 810 to model 520 (or 525, 550) with no LPAR

The source system is a model 810 with an integrated system expansion unit and no external towers. The target system is a model 520 with no external towers attached.

This is the upgrade path using migrated or converted disks:

1. Upgrade model 810 to V5R3 with the latest PTFs.
2. Ensure that there is space in the new system for a disk to be removed and relocated from the existing system unit.

**Restriction:** Model 810 has six disk slots in the base configuration, with up to 18 disks in the system unit, all running off one RAID controller IOP. A model 520 has four disk slots in the base configuration with a maximum of eight disks in the system unit.

Depending on the capacity requirements, a client can choose to house all their disks in the system unit on the 520, which may have all the eight disks on one RAID controller or four on each of the two RAID controllers. This might result in disk reconfiguration services being need to be completed prior to the upgrade.

3. Make sure that there is space for the I/O adapters to be relocated to the new server.
4. Perform a full system backup.
5. Power down the existing server.
6. Set up the Hardware Management Console (HMC).
7. Remove the disks and the I/O adapters. Ensure that you know which disk is the Load Source.
8. Plug the disks into the new system unit.
9. Install the I/O adapters in the new system.
10. Power on.
11. Fix any bus ownership issues and hardware resource naming issues.
12. Go live.

This upgrade is only complicated by disk migration issues, potentially going from 18 disks to eight, which must be performed before moving the disks across to the new system.

#### Example disk migration (Gig-Mig service)

The source system contains 18 8.58 GB disks in two RAID sets off the same IOP. These must be migrated to eight 35.16 GB disks in a single RAID set. All of the disks are in the system auxiliary storage pool (ASP).

It is assumed that the disks are 85% full. Eighteen 8.58 GB disks in two RAID sets = 137.3 GB total storage, and 85% of 137 GB = 116.7 GB of data on the system.

Perform the following tasks:

1. Perform a full system save.
2. IPL to the dedicated service tool (DST).

3. Switch off the RAID protection.
4. Remove one 8.58 GB drive from the configuration. Physically remove this drive from the system, move the load source drive to this drive's position, and place a new 35.16 GB drive into the load source position.
5. Perform a D type IPL and install SLIC (System Licensed Internal Code) in the new load source drive.
6. Perform the load source migrate procedure to migrate from the old load source drive to the new 35.16 GB drive. The old load source drive now becomes nonconfigured. (At this point, you have one 35 GB drive and 16 8 GB drives configured, and one 8 GB drive nonconfigured).
7. IPL the system to a restricted state to ensure that storage management recovery is completed.
8. IPL to DST.
9. Remove six 8.58 GB drives from the configuration. Physically remove the seven nonconfigured drives from the system and replace with seven 35.16 GB drives.

**Tip:** In this case, the ASP threshold limit will have to be increased to allow this action (defaults to 95%).

10. Initialize and format the new drives.
11. Add the new drives to the system ASP.
12. Start the RAID protection.
13. Remove the 10 remaining 8.58 GB drives from the configuration.
14. Physically remove the old drives, leaving only eight new drives.
15. Perform an IPL.

When working out a strategy for this type of data migration, it is necessary to draw up a table similar to Table 2-2. This ensures that utilization does not exceed 100%. If utilization exceeds the ASP threshold by a small amount, it is possible to temporarily increase the threshold in the system service tools (SST) in order to allow migration to occur.

*Table 2-2 Disk capacity and utilization through the migration process*

Stage	8.58 GB equivalents	35.16 GB equivalents	Disk capacity	Utilization
At start	16	0	137.28 GB	85%
Switch off RAID	18	0	155.44 GB	75%
Remove one drive from ASP	17	0	145.86 GB	80%
Migrate load source	16	1	172.44 GB	68%
Remove six 8.58 GB drives	10	1	120.96 GB	96%
Install seven 35.16 GB drives	10	8	367.08 GB	32%
Remove ten 8.58 GB drives	0	8	281.28 GB	41%

Stage	8.58 GB equivalents	35.16 GB equivalents	Disk capacity	Utilization
Start RAID	0	7	246.12 GB	47%

## 2.2.2 Model 820 with tower to model 520 (525, 550) with no LPAR

The source system is a model 820 with an integrated system expansion unit, and one #5074 external tower. The target system is a model 520 with the external tower migrated.

Follow the upgrade with a migrated or converted disks path.

1. Upgrade model 820 to V5R3 or later with the latest PTFs.
2. Ensure that there is space in the new system for the disk to be removed and relocated from the existing system unit that is maintaining the existing RAID sets.

**Restriction:** Model 820 has six disk slots in the base configuration with up to 12 disks in the system unit, all off one RAID controller IOP. A model 520 has four disk slots in the base configuration with a maximum of eight disks in the system unit.

The RAID set that contains the load source disk must be housed in the system unit (with the load source disk in slot 6). This might result in disk reconfiguration services being required prior to the upgrade.

3. Ensure that there is space for the I/O adapters to be relocated to the new server. Because the migration tower is not supported on model 520, I/O features and disks housed in this unit must be replaced before or during the upgrade.
4. Perform a full system backup.
5. Install an additional disk in the #5074 tower.
6. Install a new I/O in the #5074 tower.
7. If the system unit on the 820 contains two RAID sets, move one complete RAID set to the #5074 tower. If not, a data migration similar to that described in the previous example ("Example disk migration (Gig-Mig service)" on page 40) must be performed to get the number of disks down to the number supported in the 520 (either four or eight, depending on the order). If the system has been in use since the time you performed this action, perform another full system backup.
8. Power down the existing server.
9. Remove the disks and the I/O adapters from the system unit.
10. Set up the HMC.
11. Move the disks from the old system unit and install them in the new system unit.
12. Install the I/O adapters in the new system unit or #5074, as required.
13. Upgrade #5074 to #5094.
14. Power on the unit.
15. Fix any bus ownership issues and hardware resource naming issues.
16. Go live.



### 2.2.3 Model 640 to model 520 (or 525, 550) no LPAR

In this example, the source system, a model 640, will not upgrade to V5R3 or later. The highest release that it will support is V5R2. The upgrade process is as follows:

1. The client orders a new server. Services are ordered from IBM or an IBM Business Partner through a special bid process.
2. The new system duplicates most or all of the current environment.
3. The source system is upgraded to the highest release it can support (in this case, V5R2) to allow for interoperability.
4. The new server is installed.
5. Scratch install SLIC and base OS/400.

**Note:** The new system may be delivered with V5R3 and the licensed programs installed. In order to ensure complete system migration, scratch install the target system with only the V5R3 Licensed Internal Code and base operating system.

Refer to the section “Restoring Previous Release User Data to a New System” in *Backup and Recovery V5R4*, SC41-5304-08, which is available at:

<http://www.ibm.com/support/docview.wss?uid=pub1sc41530408>

6. Existing full system backups are used to create the new test system (using the recovery procedures outlined in *Backup and Recovery V5R4*, SC41-5304-08).
7. Upgrade the licensed programs to V5R3 or later.
8. Install the latest PTFs.
9. The client tests the current environment.
10. Any production objects that are created or altered, and are required on the new system, are saved.
11. The target server is then synchronized with the source system. This can be performed in a number of ways:
  - Installing only the changed objects (saved with the save changed objects command)
  - Installing the client data libraries only
  - Scratch installing from up-to-date source system saves

**Important:** Although scratch install is the safest way to ensure that all of the objects are synchronized, it might take an excessive amount of time.

The side-by-side method allows for an intermediate stage, where the target system is refreshed with the changed data to test the final upgrade method.

When using the save changed objects command, the client must be sure that the testing process does not change data objects. Otherwise, data mismatches might occur.

Refer to *Backup and Recovery V5R4*, SC41-5304-08 for detailed procedures.

12. Move the required hardware, if any, from the source system to the target system.
13. Perform full system backups (you require system saves in V5R4 for recovery).
14. Go live.

## 2.2.4 Model 720 to model 520 (or 525, 550)

There is no supported upgrade path from model 720 to model 520, but in this case, the source system can be upgraded to V5R3. Note that model 720 does *not* support 17 GB load source drives, and therefore, cannot have i5/OS V5R4 installed on the source system. i5/OS V5R4 must be installed during an intermediate step.

**Tip:** Because there is no supported upgrade path, the source system and the target system have different serial numbers.

If the source system never had its name changed from the shipped value, that is, Sxxxxxxx, where xxxxxxx is the system serial number, it is recommended that you do *not* copy the network attributes across, because this results in the new system being named with a serial number that is not its own.

Change the system name by issuing the CHGNETA command.

Press F4 and change any parameters as necessary.

The upgrade process is as follows:

1. The required hardware is ordered to duplicate most or all of the environment. (it is possible that the source system has communication lines that are no longer being used, and so the target system does not have to reflect the source system exactly.)
2. The source system is upgraded to V5R3.
3. The target system is installed.
4. The existing full system backups are used to create the new test system (using the recovery procedures from the Backup & Recovery guide) (iSeries - Backup and Recovery, SC41-5904-08).
5. The client tests the current environment.
6. Production objects that are created or altered, and are required on the new system, are saved.
7. The target server is then synchronized with the source system. This can be performed in a number of ways:
  - Installing only the changed objects (saved with the save changed objects command).
  - Installing only the client data libraries, assuming the program libraries are unchanged.
  - Scratch installing from up-to-date source system saves.
  - Follow the disk migration upgrade path outlined in 2.1.4, “Upgrade with converted or relocated disks” on page 38.

**Note:** Although scratch install is the safest way to ensure that all of the objects are synchronized, it might take an excessive amount of time. The method allows for an intermediate stage where the target system is refreshed with the changed data to test the final upgrade method.

When using the save changed objects command, the client must be sure that the testing process does not change the data objects. Otherwise, data mismatches occur.

Refer to *Backup and Recovery V5R4*, SC41-5304-08 for detailed procedures.

## 2.2.5 Model 840 to model 570 (system upgrade with no LPAR or Hardware Management Console)

The source system is a model 840 with a 9079 base I/O tower 9840/sb3. The target system is a model i570 with a 5294 expansion unit, using the Operations Console LAN. In this scenario, only the disks in the source system unit are moved.

**Note:** This is a disk-only migration, which has two RAID sets hanging off one RAID controller. RAID set 1 is made up of six disks, and RAID set 2 is made up of eight disks. This means that the disks can be moved straight across to the new system without any reconfiguration of disks.

Following is the upgrade process:

1. Develop an implementation plan to prepare for the upgrade, including asking the following questions:
  - Is there a supported path for the new system?
  - Is there any hardware that must be migrated or ordered?
  - Are there enough DASD capacity and slots?
  - Predefine the system console (this is important if you are planning LPARs).

**Note:** For MES upgrades, the Customized Upgrade Installation Instructions (CUII) must be used in conjunction with the implementation plan and the steps described here. These instructions are available to the hardware service representatives.

2. Upgrade model 840 to i5/OS V5R4 with the latest PTFs. This function can be performed by your hardware representative.
3. The client tests the current environment.
4. The client performs a full system backup (perform two sets, and do not forget to clean the tape drive before and after each backup).
5. Verify that all the disks are reporting in by performing the following tasks:
  - a. In the iSeries main menu, type STRSST and press Enter.
  - b. Type 1 (Start a Service Tool) and press Enter.
  - c. Type 3 (Work with disk units) and press Enter.
  - d. Type 1 (Display disk configuration status) and press Enter.

In the disk unit details display you can see the bus number, the ASP number, the serial number, and the status of the unprotected disks.

6. Print the system rack configuration using SST (STRSST):
  - a. In the iSeries main menu, type STRSST and press Enter.
  - b. Type 1 (Start a Service Tool) and press Enter.
  - c. Type 7 (Hardware Service Manager) and press Enter.
  - d. Press PF6 to print the report.
7. From the rack config list, map the resource name to the card position, for example, DD009 - D31.

**Tip:** Use the LPAR validation tool (LVT) to establish the current and the new component locations.

8. Use the rack config list, LVT report, and the diagram from the front cover panel of the source system 840 unit to locate the physical location of disk drives, and then access the

service tools (STRSST) to establish how many RAID sets were on the system. In our scenario, there were six disks in the first RAID set, and eight disks in the second RAID set. Therefore, they could be moved to the new server that maintains the RAID set.

**Note:** If you have more than six disks, including your load source in a RAID set, some additional reconfiguration tasks must be performed during the preplanning stage.

9. Verify that the Ethernet/LAN Console is in the correct slot for the Operations Console. Details about card placement are available in the topic “Operations console hardware requirements in the connecting to iSeries” on selecting **Connecting to iSeries → Operations Console → Manage Operations Console → Change from one console type to another → Twinaxial console to Operations Console**. This is available in the IBM eServer iSeries Information Center on the Web at:  
<http://www.iseries.ibm.com/infocenter>
  10. For the initial installation of the Operations Console on a LAN network, perform the following tasks:
    - a. Ensure that the PC is connected to the LAN network.
    - b. Connect the system to the LAN network using the console driver card in slot C04 or C06.
    - c. Label both the cables.
  11. Perform the following DST function to identify the Operations Console LAN PC as the system console for the DST:
    - a. Select **DST** from the IPL or Install the system menu or by selecting panel function 21.
    - b. Enter the QSECOFR user ID and password (case-sensitive) to access the DST.
    - c. Select **5** (Work with DST Environment) and press Enter.
    - d. Select **2** (System Devices) and press Enter.
    - e. Select **6** (Console Mode) and press Enter.
    - f. Select Console type **3** (Operations Console (LAN)).
    - g. Select **Save console type** by pressing F7 and store before you exit.
- Note:** This procedure is found in the section “Selecting Operations Console as the console device” in *Operations Console Setup*, SC41-5508-02.
12. When migrating to the Operations Console, it is important that you configure the new Operations Console PC before beginning the server model upgrade. At this point in the upgrade instructions, where console functions are required on the new iSeries server, you will be able to perform the required functions without your current console device. The Operations Console features matching the connectivity you plan to use must be specified as part of the order for your new iSeries server.
  13. Power down the existing system and remove the cables.
  14. Connect the new system with the HSL cables and the SPCN cables (as per the CUII document).
  15. In the new i570 system, the CE will install the catch assembly to each central electronics complex (CEC) drawer.
  16. Install the fabric flex (SMP) cable so that the left side is behind the rack frame and will not interfere with the covers or the rack trim (Figure 2-1 on page 47).



Figure 2-1 Fabric flex (SMP) cable

**Note:** Fitting the flex cable is a client install, but an MES adding a CEC drawer is considered a CE install.

17. Start with the top CEC drawer, and then align the flex cable assembly to engage the install lever with the catch assembly.
18. After ensuring that the connector pin alignment is all right, move the lever in the fabric flex cable to the installed position and lock in place. (Refer to the fabric (SMP) cable install lever action in the CUII document.)

19. Install the flexible service processor cable on the right side of the rear of the CEC unit (Figure 2-2).

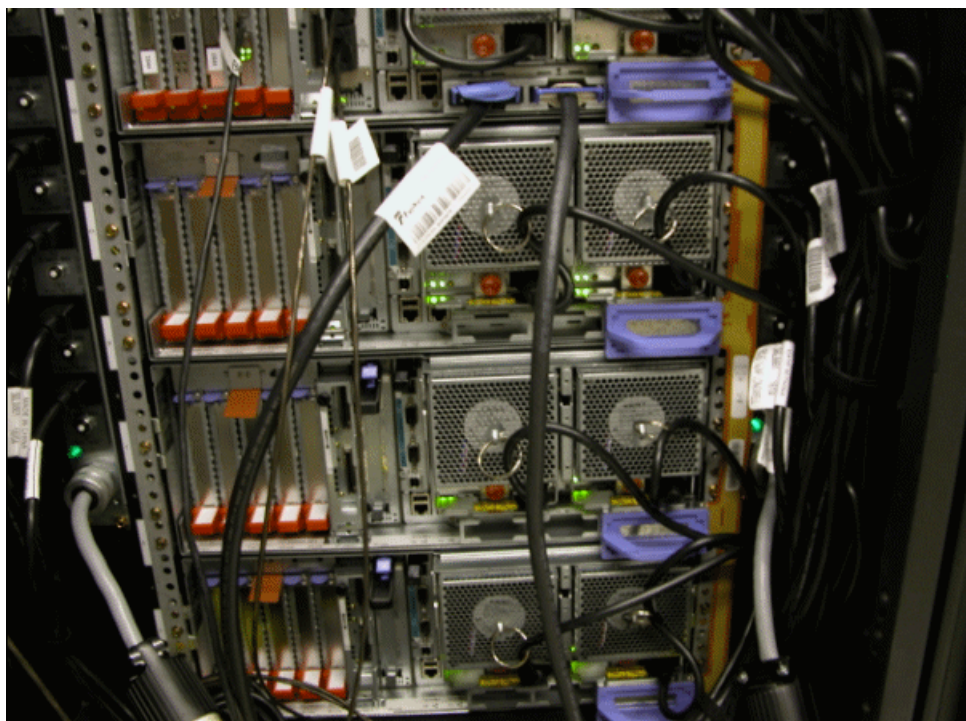


Figure 2-2 FSP cable

20. Remove the load source disk from the old server and insert it into the correct load source slot in the new system.
21. Remove the five remaining disks from the first RAID set in the old server and insert them into the empty slots in the same cage as the load source disk mentioned in the previous step (they can be placed in any order).
22. Remove the last eight disks from the second RAID set in the old server and insert them into the empty slots in the cage in the 5294 expansion unit. This maintains the existing RAID set.
23. For the first connection between the iSeries server and Operations Console PC, you must use the service tools user ID of 11111111 (eight 1s). This prevents the shipped expired user IDs from preventing a successful reauthentication of the client connection to the server. When you receive the OS/400 release upgrade, the shipped user IDs (except 11111111) are expired. To establish a successful reauthentication of the client connection to the server, use the service tools user ID of 11111111 (eight 1s). This is especially important for automatic installations.

**Attention:** Failure to comply with these actions may prevent the console from working correctly during the upgrade or install.

24. Power on the new server.
25. Perform full system backups (you require system saves in i5/OS V5R4 for recovery).
26. Go live.

**Important:** During a manual IPL of the system, if no console was specified earlier, you will receive two additional screens to confirm the setting of the console mode. The first confirmation requires F10 to accept your current console type and the second confirmation screen shows that a value did not exist previously (a zero is present against the old value) and the new value is shown. Press Enter to exit and set the console mode automatically. The IPL then continues to the IPL screen or the Install the System screen. Although this condition is most likely to occur during the installation of a new partition, it could happen on your first manual IPL of i5/OS V5R4.







## **System i5 disk at i5/OS V5R4**

This chapter describes data protection schemes that are available and the points to consider when deciding among the different schemes and the methods in which to implement them. This chapter also includes details about several ways of performing the load source disk migration that might be required when upgrading system hardware.

## 3.1 Introducing the System i5 disk technology

This section describes available methods for data protection through data redundancy techniques.

## 3.2 Disk types (speeds and feeds)

Table 3-1 shows the integrated disks that are supported on System i5.

*Table 3-1 Disk types supported for System i5*

Disk type	Capacity (GB)	Speed (rpm)
4317	8.58	10,000
4318	17.54	10,000
4319	35.16	10,000
4326	35.16	15,000
4327	70.56	15,000
4328	141.1	15,000

## 3.3 Disk packaging

In System i5, as with its predecessors, most models can accommodate disk drives in the CEC. The System i595 is the exception because it does not have any disk drive slots in the CEC.

### 3.3.1 System i 515, 525, 520, and 550

These systems all have eight disk slots that can be arranged in one or two buses, allowing either a single bus arrangement of one to eight disks or two buses that can each have one to four disks. This means the disk in the CEC can be available for one or two logical partitions. The available protection type depends on the disk adapter being used or the embedded IOP.

### 3.3.2 System i 570

The System i 570 can accommodate one to six disks in the CEC, arranged on one bus and therefore only one logical partition. These disks can use all protection types depending on the chosen disk adapter or the imbedded IOP.

### 3.3.3 System i 595

The System i 595, similar to the earlier high-end iSeries model 890, cannot have any disk drives in the CEC.

### 3.3.4 I/O expansion

The System i5 has several expansion frames that can house disk drives. These expansion frames connect to the System i5 or iSeries via the high-speed loop. The models used are the

5094, 5294 and the 5095 expansion towers. The 5294 is merely a two-high 5094. Each 5094 can house 45 disk drives and the I/O cards that drive them.

The 5095 expansion tower is a smaller unit that can be floor or rack mounted. It houses up to 12 disk units along with the I/O adapters that drive them.

A new type of disk drive draw is now available. This disk draw is available only in a 4U rack mounted enclosure. It is SCSI connected rather than HSL. This offers a longer cable length (20m) that might be attractive to customers wishing to install many disks on one system where a short HSL cable length might cause physical arrangement limitations.

The 24 drives in the EXP24 enclosure can be arranged in four six-disk packs or two 12-disk packs. These packs can be allocated to different logical partitions. The pack arrangements and protection depend on the I/O adapters controlling them. I/O adapters controlling the disk in an EXP24 can be in an I/O expansion located in the same rack as the EXP24 or the CEC.

## 3.4 Disk protection types

An i5/OS disk can have a variety of protection methods. Typically, a protection method is implemented throughout the system. However, in some instances you might choose to mix the protection types. For example, a partitioned system may have different types of protections in different partitions based on level of availability. The production partition may have mirrored protection because it requires the highest level of protection, but the development partition may have Redundant Array of Independent Disks (RAID) protection because this is a less critical environment.

The following sections provide an overview of the different protection methods.

### Unprotected

Disks can be added to auxiliary storage pools (ASPs) without any form of data protection. This method is recommended only in situations where the maximum usable disk capacity is required and data does not have to be protected, such as a system that is used only for training purposes and is regularly scratch-installed to set up new courses.

### Device parity protected

Device parity protection is a hardware function that protects data from being lost because of disk unit failure or damage to the data on a disk. Two types of device parity protections are implemented in i5/OS V5R4: RAID-5 and RAID-6. (The earlier releases of the operating system implemented only RAID-5 parity protection.)

#### *RAID-5 protection*

Disks are protected by a "parity check bit" being written for each sector on the drives. In the event of a single disk failure within a RAIDset, the system continues to operate in a degraded mode because the data in the failing unit can be calculated by using the saved parity value and the values of the bits in the same locations on the other disks.

In the event of a second disk failure within the same RAIDset, the system fails and system recovery is from data backups.

The "cost" of RAID-5 is a reduction in the overall disk capacity, equivalent to one disk per RAIDset. For example, a system with two RAID-5 RAIDsets of 10 disks each (20 drives in total) will have a total capacity equivalent to 18 disks.

A RAID-5 RAIDset can spread parity data over two, four, eight, or 16 drives. A RAID-5 RAIDset can contain a minimum of three disk drives (four for older disk input/output adapters) and a maximum of 18 disk drives.

### ***RAID-6 protection***

Disks are protected by writing two redundant data bits using the p&q parity data based on the Reed-Solomon algorithm. Conceptually, by writing two sets of parity data, a RAID-6 array can tolerate up to two disk failures within the array.

A RAID-6 array with a single disk failure is still protected as much as a RAID-5 array with no failures. A RAID-6 RAIDset with two failing drives continues to function in degraded mode until a third disk in that RAIDset fails.

The “cost” of a RAID-6 array is equivalent to two drives capacity per RAIDset. For example, a system with two RAID-6 RAIDsets of 10 disks each (20 drives) will have a total capacity equivalent to 16 disks.

RAID-6 arrays spread parity data across *all* drives in the array when RAID-6 is started, so if seven drives are in the array, they will each have two parity stripes using up a total of two-sevenths of the capacity, leaving five-sevenths of the capacity for user data. Any disk drives that are subsequently added to the array will *not* have any RAIDstripes, and so the full capacity is available for user data. (For example, adding two more drives to the RAIDset gives seven drives at five-sevenths capacity and two drives at full capacity.) For performance reasons, it is desirable to stop and restart RAID on these drives to spread the parity stripes across all the nine drives, giving nine drives of seven-ninths capacity.

A RAID-6 RAIDset can contain a minimum of four disk drives and a maximum of 18 disk drives.

RAID-6 can be implemented only on #571B and #571E IOAs, which have auxiliary cache. IOA cache is mirrored to prevent data loss in the event of an IOA cache failure.

An additional feature of RAID-6 is that when functioning with no drive failures, the RAID-6 IOA can interrogate the user data and the parity data to ensure consistency. Because of the two parity bits, any inconsistency can be isolated and corrected. For example, if a disk head is not tracking correctly, and therefore not reading data correctly, the parity bits will not conform to the data and a parity inconsistency is logged. On a RAID-5 implementation, all that is known is that there is a problem, and the failing disk cannot be isolated until other diagnostics show a hardware error. However, on a RAID-6 implementation, because of the two parity bits, the false data bits can be isolated and corrected. Thus the system can perform “data cleaning.”

**Note:** The System i5 implementation of RAID-6 uses the “P&Q parity data based on the Reed-Solomon algorithm” method. This method utilizes a hardware finite field multiplier direct memory access (DMA) engine to perform the necessary calculations. Because other implementations utilize software calculations, they use CPU capacity or have to use additional disk capacity for parity data (or both), reducing available space for the user data.

### **Mirror protected**

Disk mirroring requires each disk drive to have an identical mate. An exact copy of the data on the first drive is made to the second drive. In the event of a drive failure, the system continues to function using the other copy. The system fails only if both drives in a mirrored pair fail.

Mirror protection can be heightened by carefully selecting and placing the hardware. The system will always select the best available protection when starting the mirroring process. Mirror protection can be at the following levels, with the greatest protection coming last:

- ▶ **Disk protected**  
A disk drive failure will not cause system outage. However, because both the disks of a mirrored pair are on the same Small Computer System Interface (SCSI) bus, a failure of the SCSI bus causes system outage.
- ▶ **SCSI bus protected**  
All of the disks have their mirrored pair on a different SCSI bus. However, a mirrored pair is on the same storage adapter card (IOA). In this case, an entire SCSI bus may fail, causing the system to lose contact with all drives on that SCSI bus, and there is no system outage.
- ▶ **IOA protected**  
Both of the disks of mirrored pairs are on separate storage adapter cards (IOA). Failure of an IOA does not cause system outage.
- ▶ **Input/output processor protected**  
Mirrored pairs are separated at the input/output processor (IOP) level. Failure of an IOP does not cause system outage, although some facilities might be unavailable depending on the hardware that is also present on that IOP.
- ▶ **Bus protection**  
Mirrored pairs are separated at the system bus level. Although failure of a system bus does not cause system outage, the other hardware attached to that bus is unavailable.
- ▶ **Frame protection**  
Mirrored pairs are in separate I/O towers. Although complete failure of an I/O tower does not cause system outage, the other hardware located on that tower is unavailable.
- ▶ **High-speed link loop protection**  
Mirrored pairs are on separate high-speed link (HSL) loops. Although HSL loop failure does not cause system outage, other hardware attached to that HSL loop is unavailable.

When adding additional drives to an already mirrored system, it is necessary to stop and restart mirroring in order to gain the best level of mirroring for that hardware configuration.

### 3.4.1 RAID-5 vs RAID-6

Table 3-2 shows a comparison between RAID-5 and RAID-6.

*Table 3-2 Comparison between RAID-5 and RAID-6*

Consideration	RAID-5	RAID-6
Number of disk failures in RAIDset before system outage	1	2
Capacity cost per RAIDset (disk equivalent)	1	2
Minimum drives per RAIDset	3 (4 with older IOAs)	4
Maximum drives per RAIDset	18	18
IOA	Many different	Only #571A & #571E
Cache	Single point of failure	Auxiliary Cache (Dual Copy)

### 3.4.2 Considerations when planning disk protection

Keep these items in mind when planning your disk protection method.

#### Mixing RAID types

It is possible to mix RAID-5 and RAID-6 protection schemes on the same system, even on the same disk IOA. For example, an IOA with 12 #4327 drives and three #4328 drives connected, when deciding on the option of starting RAID-6, will start one RAID-6 RAIDset of 12 drives — each with parity stripes, and therefore having 10/12ths capacity — and one RAID-5 RAIDset of three drives. (Three drives are insufficient to start a RAID-6 RAIDset; a minimum of four drives are required.)

For operational simplicity, systems should not mix RAID types. This requirement might necessitate moving disks or buying additional hardware.

#### Auxiliary storage pools

User ASPs are designated collections of disks and are used as a method to separate data into defined areas of storage. Disks are placed in auxiliary storage pools (ASPs) during disk configuration. If disk failures occur within a user ASP that the chosen method of disk protection cannot handle, the user ASP becomes unavailable to the system. In the case of the system ASP (ASP1), this results in system outage. If a user ASP (any ASP, not ASP1) becomes unavailable, some applications continue to function if their required programs and data are not in that ASP.

User ASPs can be used for separating different applications or for performance reasons. For example, journal receivers can be placed in a user ASP so that database writes are not in contention with journal writes on the same disk.

It is advantageous to separate essential and nonessential applications into separate user ASPs and assign different levels of disk protection to each ASP. For example, archive data can be in a user ASP with RAID-5 protection, nonessential back office data in a user ASP with RAID-6 protection, and business-critical functions and data in an ASP with HSL-level mirroring.

Although it is possible to assign disks from the same RAIDset into different ASPs, careful thought must be given to the possible outcome of disk failures within the RAIDset.

#### Device types and speeds

Keep these points in mind:

- ▶ Mirrored pairs must be of the same capacity. (They can be of different speeds, but this is not recommended.)
- ▶ All of the disks in a RAIDset must be of the same capacity. (They can be of different speeds, but again, this is not recommended.)
- ▶ Load source disk for i5/OS V5R3M5 and i5/OS V5R4M0 must be 17.54 GB or higher.

#### RAID optimization

Unlike mirrored protection, all of the disk drives in a RAIDset must be on the same storage IOA card. This is because the IOA performs the calculations that are required for the parity stripes or data regeneration following disk failure. Within this limitation, there is scope for defining different optimization strategies, as outlined in the following list:

- ▶ Availability

A parity set optimized for availability offers a greater level of protection because it allows a parity set to remain functional in the event of an SCSI bus failure. The availability

optimization value ensures that a parity set is formed from at least three disk units of equal capacity, each attached to a separate bus on the IOA. For example, if an IOA has 15 disk units and is optimized for availability, the result might be five parity sets with three disk units, each attached to separate SCSI buses on the adapter. (OS/400 V5R3 is required to optimize for availability.)

- **Capacity**

A parity set that is optimized for capacity stores the maximum amount of data possible. The IOA may generate fewer parity sets with more disk units in each parity set. For example, if an I/O adapter has 15 disk units and is optimized for capacity, the result might be one parity set containing 15 disk units.

- **Balanced**

A balanced parity set compromises between the ability to store large amounts of data and to provide fast access to data. For example, if an I/O adapter has 15 disk units and you choose the balanced parity optimization, the result might be two parity sets, one with nine disk units and one with six disk units.

- **Performance**

A parity set optimized for performance provides the fastest data access. The I/O adapter might generate more parity sets with fewer numbers of disk units. For example, if an I/O adapter has 15 disk units, and is optimized for performance, the result might be three parity sets with five disk units each.

The process of selecting the RAID optimization strategy can be performed using the iSeries Navigator or the dedicated service tools (DST).

### Selecting the RAID optimization strategy using the iSeries Navigator

Perform the following tasks to select the RAID optimization strategy using the iSeries Navigator:

1. In iSeries Navigator, expand **Disk Units**, right-click **Parity Sets** and select **Change Optimization**, as shown in Figure 3-1.

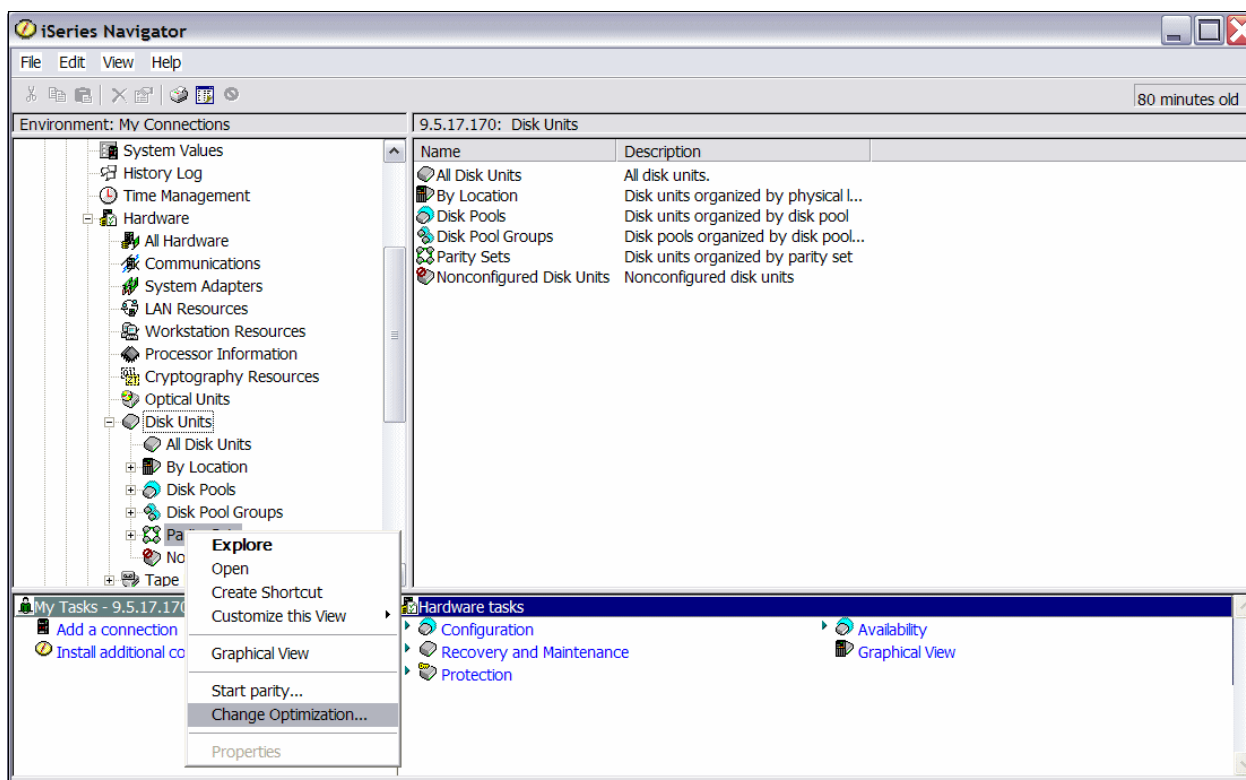


Figure 3-1 Changing RAID optimization using iSeries Navigator



2. In the page that is displayed (Figure 3-2), use the Optimization drop-down box to select the required optimization.

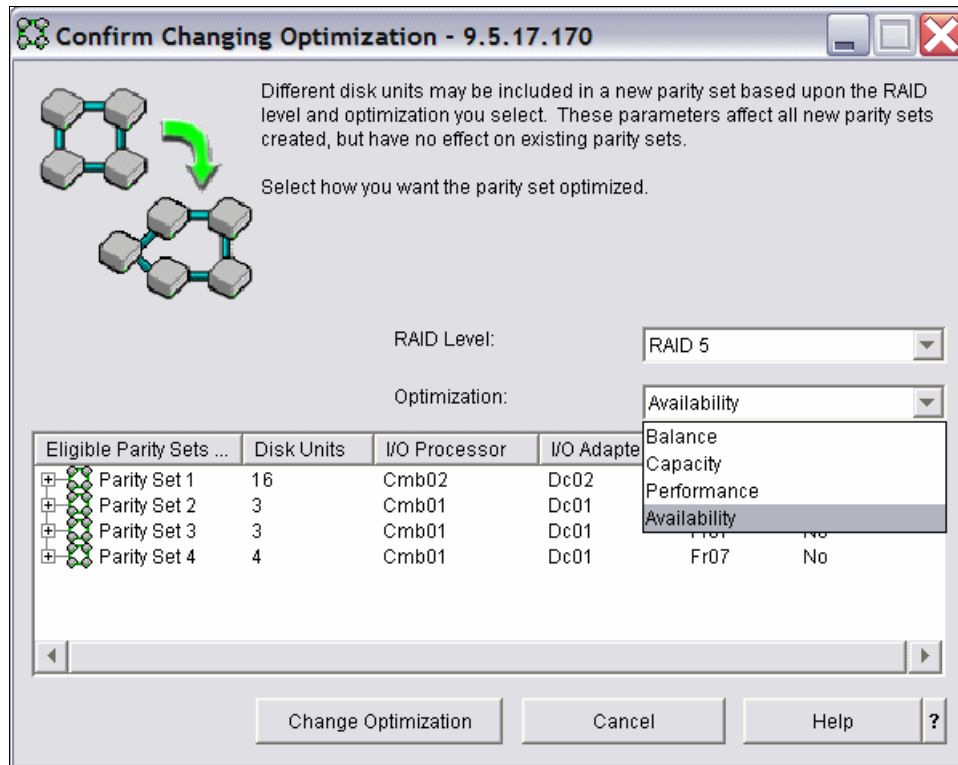


Figure 3-2 Selecting optimization

3. On the same page use the RAID Level drop-down box to select the required RAID type, as shown in Figure 3-3. Click **Change Optimization**.

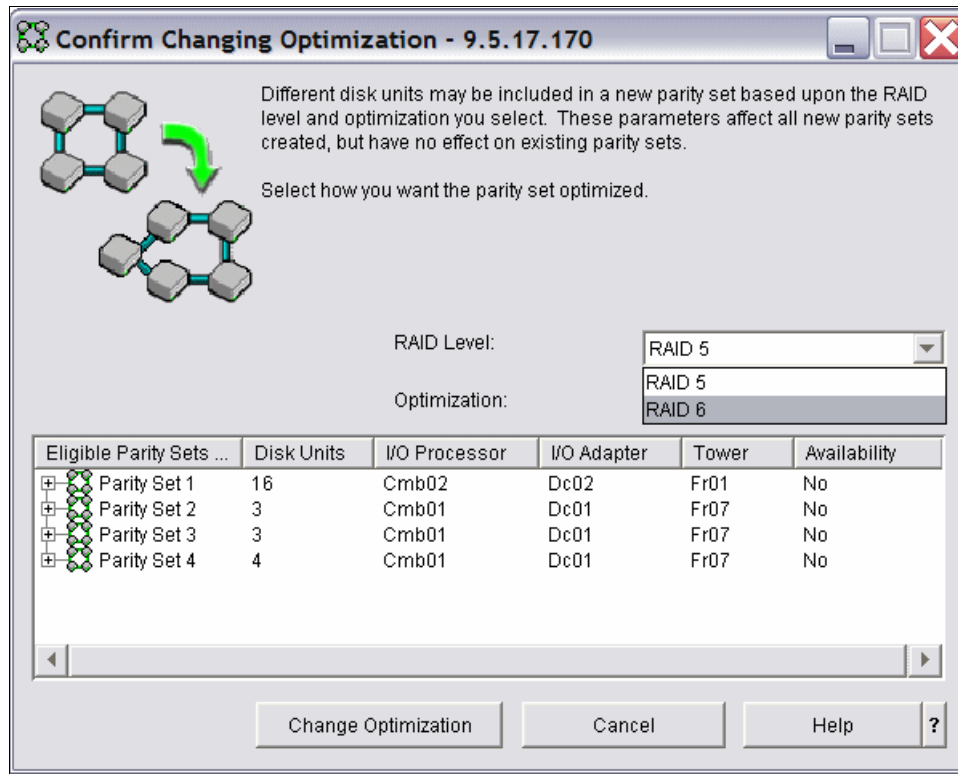


Figure 3-3 Changing the RAID Level

### ***Selecting RAID optimization strategy using the dedicated service tools***

Perform the following tasks to select the RAID optimization strategy using the DST:

1. In the DST main menu, select **Work with Disk Units**.
2. Select **Work with Disk Configuration**.
3. Select **Work with device parity protection**.
4. The screen in Figure 3-4 appears. Enter 7 for Select parity optimization.

Work with Device Parity Protection

Select one of the following:

1. Display device parity status
2. Start device parity protection - RAID 5
3. Stop device parity protection
4. Include unit in device parity protection
5. Exclude unit from device parity protection
6. Start device parity protection - RAID 6
7. Select parity optimization

Selection

-

F3=Exit                  F12=Cancel

*Figure 3-4 Changing RAID optimization using DST*

5. In the Select Parity Optimization screen (Figure 3-5), select the required type of optimization and press Enter.

```

                                Select Parity Optimization

Select how you want the parity set optimized:

The current parity optimization is:  Balanced

Type choice, press Enter.
  Select parity optimization

      1. Availability
      2. Balance
      3. Capacity
      4. Performance

Selection
      ↵

F3=Exit      F12=Cancel

```

Figure 3-5 Selecting parity optimization

If the required optimization cannot be performed due to resource constraints (for example, not enough disks), a message is displayed when starting RAID, as shown in Figure 3-6.

```

                                Parity set will not have high availability

You have selected the High Availability configuration
optimization for device parity, but the parity sets
listed below will not be configured for High Availability.
There must be one disk unit of the same capacity attached
to each Input/Output Adapter (IOA) to achieve the
High Availability configuration

If you proceed, the following parity sets will not have
the High Availability configuration.
Parity  Serial                      Resource
Set    Number      Type   Model  Name
  1    0C-6200013   571F   001    DC02
  2    0C-6199036   571B   001    DC01
  3    0C-6199036   571B   001    DC01
  4    0C-6199036   571B   001    DC01

F3=Exit      F12=Cancel
Function key not allowed

```

Figure 3-6 Error message due to inadequate disks being available for the selected optimization

After RAID is started with the required optimization, the Display Device Parity Status screen (Figure 3-7) displays information about the optimization used.

Display Device Parity Status							
Parity Set	ASP	Unit	Serial Number	Type	Model	Resource Name	Status
4	*	*	68-0E30697	4326	070	DD023	Active
	*	*	68-0E306CE	4326	078	DD025	Active
			0C-6199036	571B	001	DC01	RAID-5
	*	*	68-0E2E116	4327	078	DD017	Active
	*	*	68-0E2C3DD	4327	078	DD019	Active
5	*	*	68-0E3F6F8	4327	070	DD018	Active
			0C-6199036	571B	001	DC01	RAID-6/Availability
	*	*	21-89B8D	4328	099	DD033	Active
	*	*	21-89BA7	4328	099	DD021	Active
	*	*	21-89C7A	4328	099	DD020	Active
	*	*	21-89C42	4328	099	DD032	Active
							Bottom
* - See help for more information							
Press Enter to continue.							
F3=Exit		F5=Refresh		F9=Display disk unit details			
F11=Display disk hardware status		F12=Cancel					

Figure 3-7 Display device parity information screen

### 3.4.3 Migrating to RAID-6 from unprotected disk with iSeries Navigator

To migrate to RAID-6 from unprotected disk with iSeries Navigator, follow these steps:

1. In iSeries Navigator, expand **Disk Units**, right-click **Parity Sets** and select **Start parity**.

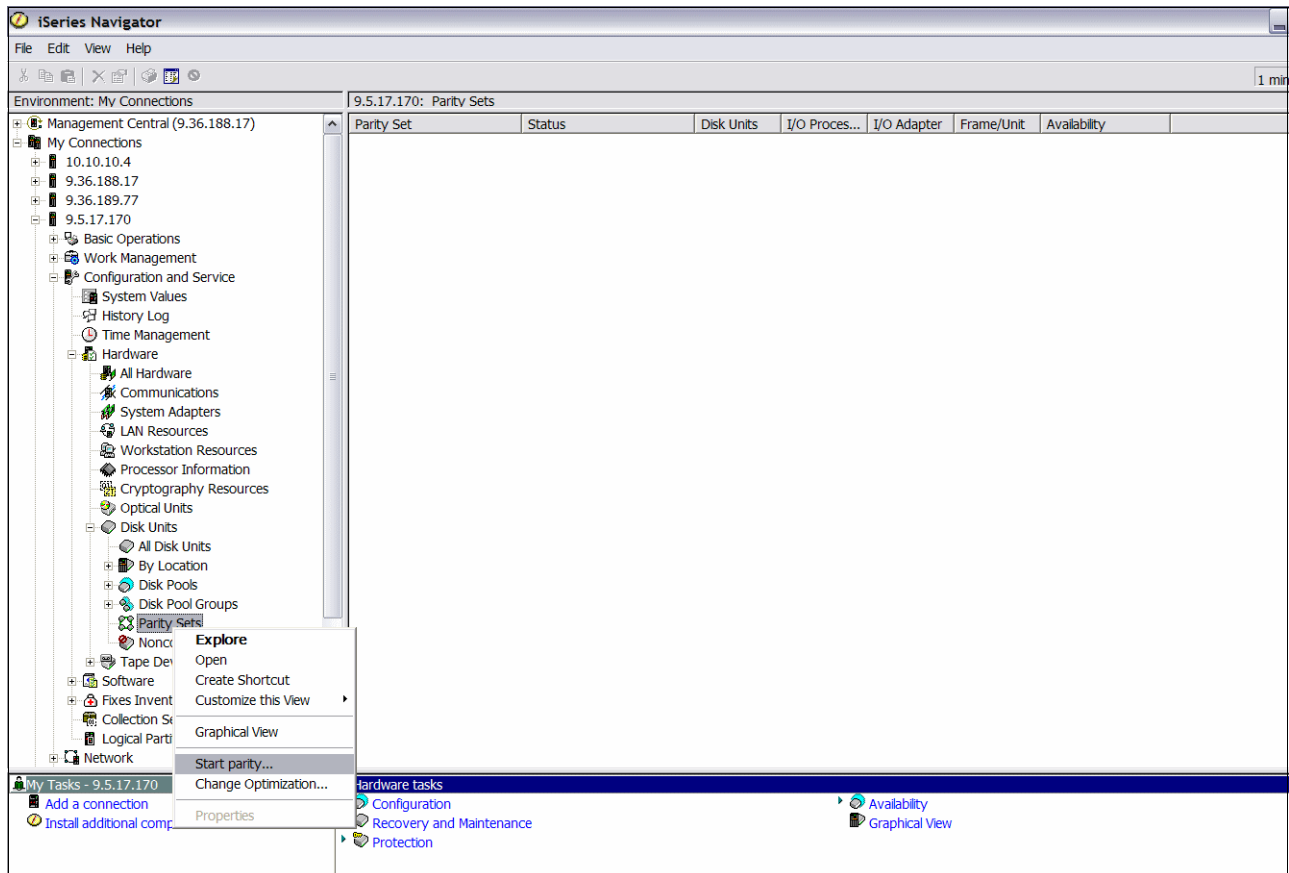


Figure 3-8 Selecting Start parity from Operations Navigator

2. On the page that is displayed (Figure 3-9), confirm that the RAID Level and Optimization settings are correct. Select the boxes for the RAIDsets you want to start, and click **Start Parity**.

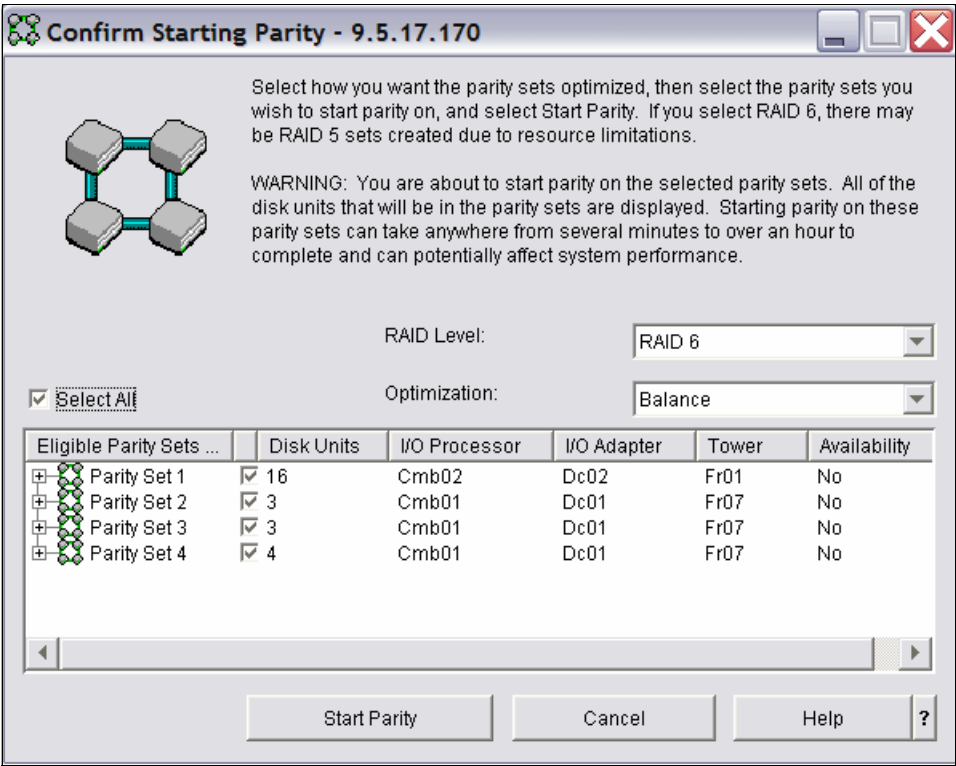


Figure 3-9 The Confirm Starting Parity window

The Start Parity status window appears (Figure 3-10).

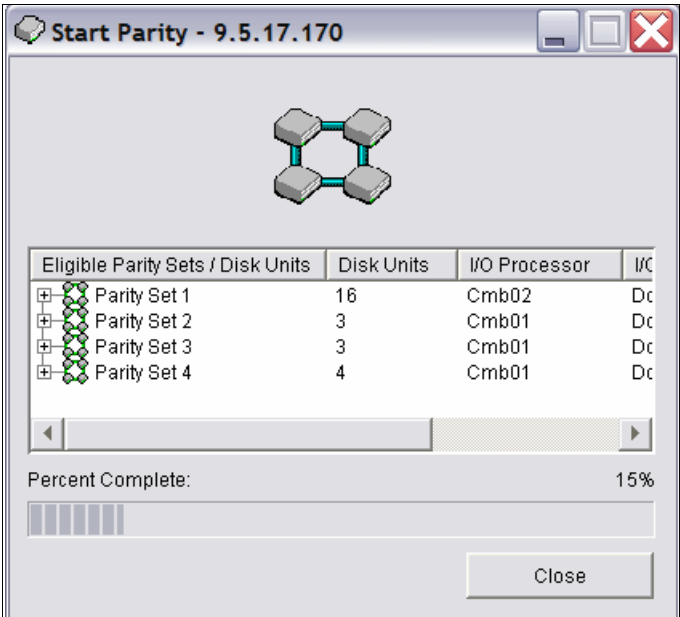


Figure 3-10 The Start Parity status window

### 3.4.4 Migrating to RAID-6 from unprotected disk using dedicated service tools

To migrate to RAID-6 from unprotected disk using the DST, follow these steps:

1. From the DST main menu, select **Work with Disk Units**.
2. Select **Work with disk unit configuration**.
3. Select **Work with Device Parity Protection**.
4. On the screen shown in Figure 3-11, enter 6 for **Start device Parity Protection - RAID-6**.

Work with Device Parity Protection

Select one of the following:

1. Display device parity status
2. Start device parity protection - RAID 5
3. Stop device parity protection
4. Include unit in device parity protection
5. Exclude unit from device parity protection
6. Start device parity protection - RAID 6
7. Select parity optimization

Selection

-

F3=Exit      F12=Cancel

Figure 3-11 Working with device parity protection in DST



5. If there are insufficient drives for RAID-6, the system automatically selects RAID-6 where possible, and RAID-5 where alternately possible (Figure 3-13). If there are only two disks of a particular size on an ASP, they will remain unprotected. In the Start Device Parity Protection screen (Figure 3-12), select the RAIDsets you want to start and press Enter.

```

                                Start Device Parity Protection

Select the subsystems to start device parity protection.

Type choice, press Enter.
1=Start device parity protection

Option   RAID   Parity   Serial   Type   Resource
         Level Set   Number
-         RAID-5  1       0C-6200013  571F  DC02
-         RAID-5  2       0C-6199036  571B  DC01
-         RAID-5  3       0C-6199036  571B  DC01
-         RAID-5  4       0C-6199036  571B  DC01

F3=Exit      F12=Cancel

```

Figure 3-12 The Start Device Parity Protection screen

```

                                Start Device Parity Protection

Select the subsystems to start device parity protection.
Some RAID-5 sets were selected due to resource limitations.

Type choice, press Enter.
1=Start device parity protection

Option   RAID   Parity   Serial   Type   Resource
         Level Set   Number
-         RAID-6  1       0C-6200013  571F  DC02
-         RAID-5  2       0C-6199036  571B  DC01
-         RAID-5  3       0C-6199036  571B  DC01
-         RAID-6  4       0C-6199036  571B  DC01

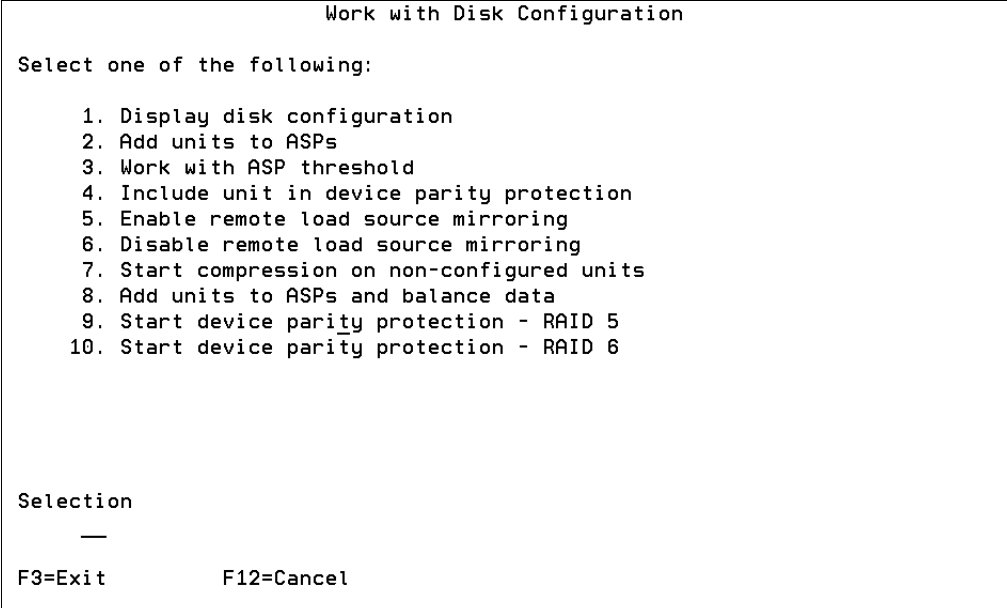
F3=Exit      F12=Cancel

```

Figure 3-13 Start device parity protection selection screen at DST

### 3.4.5 Migrating to RAID-6 from unprotected disk using system service tools

The system service tools (SST) menu (Figure 3-14) is similar to the DST menu. The actions to be performed in SST are similar to those actions described for DST in the earlier sections.



```
Work with Disk Configuration

Select one of the following:

    1. Display disk configuration
    2. Add units to ASPs
    3. Work with ASP threshold
    4. Include unit in device parity protection
    5. Enable remote load source mirroring
    6. Disable remote load source mirroring
    7. Start compression on non-configured units
    8. Add units to ASPs and balance data
    9. Start device parity protection - RAID 5
   10. Start device parity protection - RAID 6

Selection
  _____

F3=Exit      F12=Cancel
```

Figure 3-14 Working with the disk configuration screen in SST

### 3.4.6 Migrating to RAID-6 from mirrored

To change the disk protection from mirrored to RAID-6, follow these steps:

1. IPL to DST.
2. Stop Mirroring.
3. Start RAID-6.

### 3.4.7 Migrating to RAID-6 from RAID-5 protected

To change to protection from RAID-5 to RAID-6, follow these steps:

1. IPL to DST.
2. Stop RAID-5.
3. Start RAID-6.

## 3.5 Load source migration

The load source drive for a system or logical partition (LPAR) must be at least 4.19 GB for i5/OS V5R3, and at least 17.54 GB for i5/OS V5R3M5 and i5/OS V5R4M0. For a better performance, the faster 15,000 revolutions per minute (rpm) drives are recommended.

When upgrading a system to System i5, it is therefore often necessary to migrate the load source data from a small drive to a larger drive. When moving to System i5 hardware, this stage of the upgrade usually takes place on the old (preupgrade) system, but may take place on the new (postupgrade) system if both drives are supported.

The load source migration is not a part of the upgrade, and as such, is a chargeable service performed by an IBM customer engineer (CE) or IBM Business Partner.

### Usual system upgrade task sequence

This is the sequence of events in a usual system upgrade task:

1. Migrate the Load Source.
2. Upgrade the operating system and install the program temporary fix (PTF).
3. Upgrade the system hardware.
4. Perform disk and I/O reconfiguration.

This sequence might have to be altered if hardware that not being supported in the release is in use. For example, the operating system might have to be upgraded and PTFs applied before load source migration because the new load source disk might not be supported in the current release.

If moving from 8xx hardware, your new load source drive might be larger than is supported on your current system. In such a situation, you must either perform the upgrade as an “unload - reload” or upgrade the load source to a 17 GB drive on your current system, then perform another load source upgrade on your target (upgraded) system to the larger drive.

### 3.5.1 Considerations for load source migration

Keep the following issues in mind when performing load source migration:

- ▶ The target load source (LS) drive must be equal or greater in usable capacity than the source LS drive.
- ▶ The hardware level and the operating system level of the host system for the process must support both the source LS drive and the target LS drive.
- ▶ *Always* perform a full system save before starting the process.
- ▶ When moving RAID-protected drives, all of the drives in a RAIDset must move together when moving between storage IOAs.
- ▶ Check the number of drive bays in the target system; they might be less than the number of bays in the source system. For example, if you are moving from model 800 to model 520, there might be six drives in the load source disk's RAIDset in model 800, but only four disk positions in the CEC of model 520.
- ▶ Draw a map of all drives that will be moved and record their serial numbers and positions. iSeries Navigator provides a useful graphical representation of disks and their positions.

When moving disks to the PCI-X IOAs from the non-PCI-X IOAs, the RAID arrangement on disk physically changes at the next IPL. This re-arrangement process is non-reversible.

**Note:** The process is basically the same for a system with an LPAR as for a system without an LPAR. All you have to do is follow the relevant scenario instructions.

### 3.5.2 Load source migration: No disk protection

This process assumes no RAID or mirroring disk protection. Follow these steps:

1. Perform a full system save.
2. Power down the system.
3. Install the new drive in the system. Remove an existing drive, if necessary.
4. Change the mode to Manual and IPL to DST.
5. In the next screen (Figure 3-15), enter 3 (Use Dedicated Service Tools).

```
IPL or Install the System                                System:  S10E80CC

Select one of the following:

    1. Perform an IPL
    2. Install the operating system
    3. Use Dedicated Service Tools (DST)
    4. Perform automatic installation of the operating system
    5. Save Licensed Internal Code

Selection
-

Licensed Internal Code - Property of IBM 5722-999 Licensed
Internal Code (c) Copyright IBM Corp. 1980, 2006. All
rights reserved. US Government Users Restricted Rights -
Use duplication or disclosure restricted by GSA ADP schedule
Contract with IBM Corp.
```

Figure 3-15 The IPL or Install the System screen

6. In the Dedicated Service Tools screen, sign in to DST as QSECOFR (Figure 3-16).

**Note:** The DST QSECOFR password is not the same as the QSECOFR user ID password, and is case-sensitive.

```

                                Dedicated Service Tools (DST) Sign On
                                System:   S10E80CC
Type choices, press Enter.

Service tools user . . . . . qsecofr
Service tools password . . . . .

```

Figure 3-16 Signing in to DST

7. In the Use Dedicated Service Tools (DST) screen (Figure 3-17), enter 4 (Work with disk units).

```

                                Use Dedicated Service Tools (DST)
                                System:   S10E80CC
Select one of the following:

1. Perform an IPL
2. Install the operating system
3. Work with Licensed Internal Code
4. Work with disk units
5. Work with DST environment
6. Select DST console mode
7. Start a service tool
8. Perform automatic installation of the operating system
9. Work with save storage and restore storage
10. Work with remote service support
11. Work with system partitions
12. Work with system capacity
13. Work with system security
14. End batch restricted state

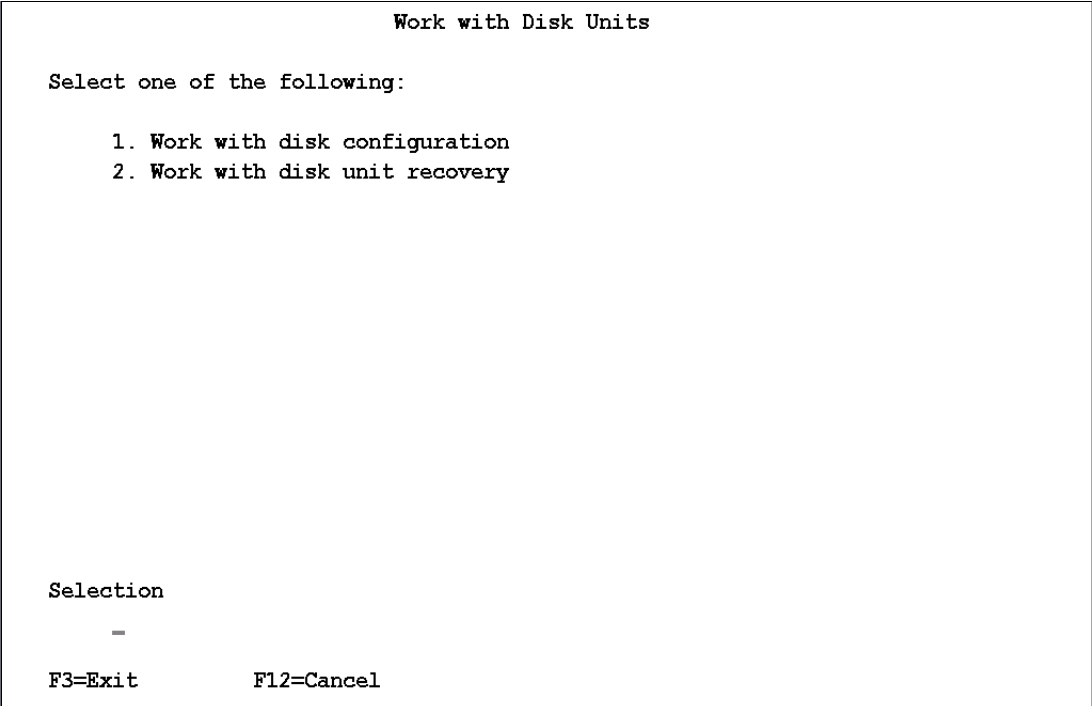
Selection
    _

F3=Exit  F12=Cancel

```

Figure 3-17 The Use Dedicated Service Tools (DST) screen

8. In the Work with Disk Units screen (Figure 3-18), enter 2 (Work with disk unit recovery).



```
Work with Disk Units

Select one of the following:

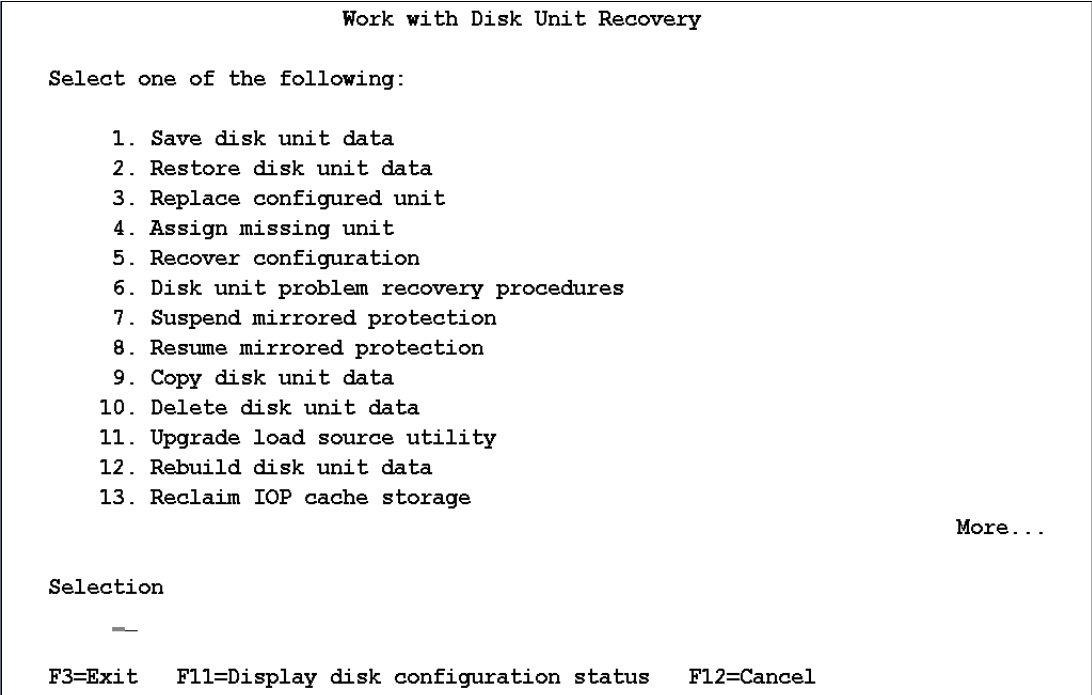
    1. Work with disk configuration
    2. Work with disk unit recovery

Selection
    -

F3=Exit      F12=Cancel
```

Figure 3-18 The Work with Disk Units screen

9. In the Work with Disk Unit Recovery screen (Figure 3-19), enter 6 (Disk unit problem recovery procedures).



```
Work with Disk Unit Recovery

Select one of the following:

    1. Save disk unit data
    2. Restore disk unit data
    3. Replace configured unit
    4. Assign missing unit
    5. Recover configuration
    6. Disk unit problem recovery procedures
    7. Suspend mirrored protection
    8. Resume mirrored protection
    9. Copy disk unit data
   10. Delete disk unit data
   11. Upgrade load source utility
   12. Rebuild disk unit data
   13. Reclaim IOP cache storage

More...

Selection
    -

F3=Exit  F11=Display disk configuration status  F12=Cancel
```

Figure 3-19 The Work with Disk Unit Recovery screen

10. In the Disk Unit Problem Recovery Procedures screen (Figure 3-20), enter 1 (Initialize and format disk unit).

Disk Unit Problem Recovery Procedures	
Select one of the following:	
1. Initialize and format disk unit	
2. Display/change page data	
3. Analyze disk unit surface	
Selection	
-	
F3=Exit    F11=Display disk configuration status    F12=Cancel	

Figure 3-20 The Disk Unit Problem Recovery Procedures screen

11. In the screen that is displayed, select the new nonconfigured drive to initialize and confirm.
12. Return to the Work with Disk Unit Recovery screen (Figure 3-19 on page 72) and enter 9 (Copy disk unit data).
13. In the screen that is displayed (Figure 3-21), select the load source disk unit (disk unit 1) as the unit to copy.

Select Copy from Disk Unit																														
Type option, press Enter.																														
1=Select																														
<table><thead><tr><th colspan="2"></th><th colspan="2">Serial</th><th colspan="2">Resource</th><th></th></tr><tr><th>OPT</th><th>Unit</th><th>ASP</th><th>Number</th><th>Type</th><th>Model</th><th>Name</th><th>Status</th></tr></thead><tbody><tr><td>-</td><td>1</td><td>1</td><td>68-0E1F75A</td><td>4326</td><td>050</td><td>DD002</td><td>Active</td></tr></tbody></table>										Serial		Resource			OPT	Unit	ASP	Number	Type	Model	Name	Status	-	1	1	68-0E1F75A	4326	050	DD002	Active
		Serial		Resource																										
OPT	Unit	ASP	Number	Type	Model	Name	Status																							
-	1	1	68-0E1F75A	4326	050	DD002	Active																							
F3=Exit    F5=Refresh    F11=Display non-configured units    F12=Cancel																														

Figure 3-21 The Select Copy from Disk Unit screen

14. In the Select Copy to Disk Unit Data screen (Figure 3-22), select the nonconfigured unit that you installed in step 3 on page 70 as the unit to copy to.

Select Copy to Disk Unit Data

Disk being copied:

Unit	ASP	Serial Number	Type	Model	Resource Name	Status
1	1	68-0E1F75A	4326	050	DD002	Active

1=Select

Option	Serial Number	Type	Model	Resource Name	Status
-	68-0E35989	4327	050	DD004	Non-configured
-	68-0E38897	4327	050	DD003	Non-configured

F3=Exit    F11=Display disk configuration status    F12=Cancel

Figure 3-22 The Select Copy to Disk Unit Data screen

15. This displays the Copy Disk Unit Data Status screen (Figure 3-23).

Copy Disk Unit Data Status

-

The operation to copy a disk unit will be done in several phases. The phases are listed here and the status will be indicated when known.

Phase	Status
Stop compression (if needed) . . . . .	Completed
Prepare disk unit . . . . .	4 % Complete
Start compression (if needed) . . . . .	
Copy status. . . . .	

Number of unreadable pages:

Figure 3-23 The Copy Disk Unit Data Status screen

16. Wait for copy to complete.
17. Power off the system.
- From the DST main screen (Figure 3-17 on page 71), enter 7 (Start a service tool),
  - Or on the Service tools screen, enter 7 (Operator panel functions).



When you see the screen in Figure 3-24, press F10 to power off.

Operator Panel Functions		System: RCHASM05
IPL source:	<u>2</u> (1=A, 2=B or 3=D)	
IPL mode:	<u>1</u> (1=Manual, 2=Normal, 3=Secure or 4=Auto)	
Press Enter to change the IPL attributes and return to the main DST menu.		
Press F8 to set the IPL attributes and restart the system. Machine processing will be ended and the system will be restarted.		
Press F10 to set the IPL attributes and power off the system. Machine processing will be ended and the system will be powered off.		
Press F12 to return to the main DST menu without changing IPL attributes.		
F3=Exit F8=Restart F10=Power off F12=Cancel		

Figure 3-24 The Operator Panel Functions screen

18. Find the old load source disk unit and slide the disk unit out of the system.
19. Move the new load source disk to the load source position.
20. If you removed a drive in step 3 on page 70, reinstall it.
21. Perform an IPL on the system.

### 3.5.3 Load source migration: Mirrored system

This section describes load source migration of a mirrored system.

**Notes:** Ensure that you record the serial numbers and the locations at relevant points.

Be *very* careful when repositioning disks. Wrong placement of disks can lead to unpredictable results and might require a full system reload from the backup tapes.

Follow these steps:

1. Perform a full system save.
2. Locate the load source unit (Unit 1) and its mirrored pair, and make a note of the locations and the serial numbers of the drives.
3. Power down the system.
4. Install the two new disk drives. Note the serial numbers of the drives and their positions.
5. Perform an IPL in manual mode to the DST.

6. Suspend the load source mate as follows:
  - a. On the IPL or the Install the System screen (Figure 3-25), enter 3 (Use dedicated Service Tools).

IPL or Install the System	
Select one of the following: <ol style="list-style-type: none"> <li>1. Perform an IPL</li> <li>2. Install the operating system</li> <li>3. Use Dedicated Service Tools (DST)</li> <li>4. Perform automatic installation of the operating system</li> <li>5. Save Licensed Internal Code</li> </ol>	System:
Selection	
-	
Licensed Internal Code - Property of IBM 5722-999 Licensed Internal Code (c) Copyright IBM Corp. 1980, 2004. All rights reserved. US Government Users Restricted Rights - Use duplication or disclosure restricted by GSA ADP schedule Contract with IBM Corp.	

Figure 3-25 The IPL or Install the System screen

- b. Sign in to the DST (Figure 3-26).

Dedicated Service Tools (DST) Sign On	
Type choices, press Enter.	System:
Service tools user . . . . .	_____
Service tools password . . . . .	

Figure 3-26 Signing in to the DST

- c. On the DST main menu (Use Dedicated Service Tools screen shown in Figure 3-27), enter 4 (Work With Disk Units).

Use Dedicated Service Tools (DST)	
	System:
Select one of the following:	
<ul style="list-style-type: none"><li>1. Perform an IPL</li><li>2. Install the operating system</li><li>3. Work with Licensed Internal Code</li><li>4. Work with disk units</li><li>5. Work with DST environment</li><li>6. Select DST console mode</li><li>7. Start a service tool</li><li>8. Perform automatic installation of the operating system</li><li>9. Work with save storage and restore storage</li><li>10. Work with remote service support</li><li>11. Work with system partitions</li> <li>13. Work with system security</li><li>14. End batch restricted state</li></ul>	
Selection	
—	
F3=Exit    F12=Cancel	

Figure 3-27 The DST main menu

- d. On the Work with Disk Units screen (Figure 3-28), enter 2 (Work with disk unit recovery).

Work with Disk Units
Select one of the following:
<ul style="list-style-type: none"><li>1. Work with disk configuration</li><li>2. Work with disk unit recovery</li></ul>

Figure 3-28 The Work with Disk Units screen

- e. On the Work with Disk Unit Recovery screen (Figure 3-29), enter 7 (Suspend mirrored protection).

Work with Disk Unit Recovery

Select one of the following:

1. Save disk unit data
2. Restore disk unit data
3. Replace configured unit
4. Assign missing unit
5. Recover configuration
6. Disk unit problem recovery procedures
7. Suspend mirrored protection
8. Resume mirrored protection
9. Copy disk unit data
10. Delete disk unit data
11. Upgrade load source utility
12. Rebuild disk unit data
13. Reclaim IOP cache storage

More...

Selection

—

F3=Exit    F11=Display disk configuration status    F12=Cancel

Figure 3-29 The Work with Disk Unit Recovery screen

- f. At the Suspend Mirrored Protection screen (Figure 3-30), select unit 1 (the load source mate).

Suspend Mirrored Protection

Type option, press Enter.

1=Suspend Mirrored Protection

OPT	Unit	ASP	Serial Number	Type	Model	Resource Name	Status
—	1	1	75-0CE64B0	6717	050	DD001	Active
—	2	1	75-0D7B2A2	6718	050	DD003	Active
—	2	1	75-0D7EDB4	6718	050	DD002	Active

F3=Exit                  F5=Refresh                  F12=Cancel

Figure 3-30 The Suspend Mirrored Protection screen

7. Copy the load source disk unit data to one of the new drives as follows:
  - a. At the Work with Disk Unit Recovery screen (Figure 3-31), enter 6 (Copy Disk Unit Data).

Work with Disk Unit Recovery

Select one of the following:

1. Save disk unit data
2. Restore disk unit data
3. Replace configured unit
4. Assign missing unit
5. Recover configuration
6. Disk unit problem recovery procedures
7. Suspend mirrored protection
8. Resume mirrored protection
9. Copy disk unit data
10. Delete disk unit data
11. Upgrade load source utility
12. Rebuild disk unit data
13. Reclaim IOP cache storage

More...

Selection

—

F3=Exit    F11=Display disk configuration status    F12=Cancel

Figure 3-31 The Work with Disk Unit Recovery screen

- b. At the Select Copy from Disk Unit screen (Figure 3-32), select unit 1.

Select Copy from Disk Unit

Type option, press Enter.

1=Select

OPT	Unit	ASP	Serial Number	Type	Model	Resource Name	Status
—	1	1	75-0CF43A4	6717	050	DD006	Active

F3=Exit    F5=Refresh    F11=Display non-configured units    F12=Cancel

Figure 3-32 The Select Copy from Disk Unit screen

- c. Select one of the new drives on the Select Copy to Disk Unit screen (Figure 3-33) and note the serial number.

Select Copy to Disk Unit Data

Disk being copied:

Unit	ASP	Serial Number	Type	Model	Resource Name	Status
1	1	75-0CF43A4	6717	050	DD006	Active

1=Select

Option	Serial Number	Type	Model	Resource Name	Status
<u>1</u>	68-0C82161	6718	050	DD004	Non-configured
-	68-0C231E9	6718	050	DD005	Non-configured

F3=Exit    F11=Display disk configuration status    F12=Cancel

Figure 3-33 The Select Copy to Disk Unit Data screen

- d. Press F10 to accept the warning “Other disk unit will become missing”.
- e. Press Enter to confirm the copy.

The Copy Disk Unit Data Status screen (Figure 3-34) appears.

Copy Disk Unit Data Status

The operation to copy a disk unit will be done in several phases. The phases are listed here and the status will be indicated when known.

Phase	Status
Stop compression (if needed) . . . . .	Completed
Prepare disk unit . . . . .	3 % Complete
Start compression (if needed) . . . . .	
Copy status. . . . .	

Number of unreadable pages:

Figure 3-34 The Copy Disk Unit Data Status screen

8. Return to the DST main screen (Figure 3-35) and power down the system (or partition) as follows:
- Enter 7 (Start a service tool).

Use Dedicated Service Tools (DST)	
	System:
Select one of the following:	
<ol style="list-style-type: none"><li>1. Perform an IPL</li><li>2. Install the operating system</li><li>3. Work with Licensed Internal Code</li><li>4. Work with disk units</li><li>5. Work with DST environment</li><li>6. Select DST console mode</li><li>7. Start a service tool</li><li>8. Perform automatic installation of the operating system</li><li>9. Work with save storage and restore storage</li><li>10. Work with remote service support</li><li>11. Work with system partitions</li><li>13. Work with system security</li><li>14. End batch restricted state</li></ol>	
Selection	
—	
F3=Exit F12=Cancel	

Figure 3-35 The DST main screen

- At the screen shown in Figure 3-36, enter 7 (Operator panel functions).

Start a Service Tool	
	System:
Attention: Incorrect use of this service tool can cause damage to data in this system. Contact your service representative for assistance.	
Select one of the following:	
<ol style="list-style-type: none"><li>1. Display/Alter/Dump</li><li>2. Licensed Internal Code log</li><li>3. Trace Licensed Internal code</li><li>4. Hardware service manager</li><li>5. Main storage dump manager</li><li>6. Product activity log</li><li>7. Operator panel functions</li><li>8. Performance data collector</li></ol>	
Selection	
—	
F3=Exit F12=Cancel	

Figure 3-36 The Start a Service Tool screen

- c. On the Operator Panel Functions screen (Figure 3-37), press F10 to power off.

Operator Panel Functions		System:
IPL source:	<u>2</u>	(1=A, 2=B or 3=D)
IPL mode:	<u>1</u>	(1=Manual, 2=Normal, 3=Secure or 4=Auto)
Press Enter to change the IPL attributes and return to the main DST menu.		
Press F8 to set the IPL attributes and restart the system. Machine processing will be ended and the system will be restarted.		
Press F10 to set the IPL attributes and power off the system. Machine processing will be ended and the system will be powered off.		
Press F12 to return to the main DST menu without changing IPL attributes.		
F3=Exit    F8=Restart    F10=Power off    F12=Cancel		

Figure 3-37 The Operator Panel Functions screen

9. Remove the load source drive (the serial number and location you noted in step 2 on page 75) from the system.
10. Move the new load source drive (the serial number and location you noted in step 7 on page 79) to that slot.
11. Remove the old load source mate (the serial number you noted in step 2 on page 75).
12. Move the new load source mate to that slot (the serial number and location you noted in step 7 on page 79).
13. Power on the system (or partition) in manual mode.



14. Replace the configured unit as follows:
  - a. Sign on to the DST.
  - b. Select the option for Work with Disk Units.
  - c. Select the option for Work with Disk Unit Recovery.
  - d. At the screen shown in Figure 3-38, enter 3 (Replace configured unit).

Work with Disk Unit Recovery

Select one of the following:

1. Save disk unit data
2. Restore disk unit data
3. Replace configured unit
4. Assign missing unit
5. Recover configuration
6. Disk unit problem recovery procedures
7. Suspend mirrored protection
8. Resume mirrored protection
9. Copy disk unit data
10. Delete disk unit data
11. Upgrade load source utility
12. Rebuild disk unit data
13. Reclaim IOP cache storage

More...

Selection

—

F3=Exit    F11=Display disk configuration status    F12=Cancel

Figure 3-38 The Work with Disk Unit Recovery screen

- e. Enter 1 next to the suspended Unit 1 disk unit at the screen shown in Figure 3-39.

Select Configured Unit to Replace

Type option, press Enter.

1=Select

OPT	Unit	ASP	Serial Number	Type	Model	Resource Name	Status
—	1*	1	75-0CE64B0	6717	050	DD001	Suspended

F3=Exit            F5=Refresh            F12=Cancel

Figure 3-39 The Select Configured Unit to Replace screen

- f. At the Select Replacement Unit screen (Figure 3-40), enter 1 next to the newly installed disk unit, and press Enter to confirm.

```

Select Replacement Unit

Unit  ASP  Serial      Type  Model  Resource  Status
      1*   1  75-0CE64B0  6717   050   DD001     Suspended

Type option, press Enter.
1=Select

Option  Serial      Type  Model  Resource  Status
      1  68-0C231E9  6718   050   DD005     Non-configured

F3=Exit      F12=Cancel

```

Figure 3-40 The Select Replacement Unit screen

The status is displayed in the Replace Disk Unit Data Status screen (Figure 3-41).

```

Replace Disk Unit Data Status

The operation to replace a disk unit from the selected disk
units will be done in several phases. The phases are listed
here and the status will be indicated when known.

Phase                                     Status

Stop compression (if needed) . . . . . : Completed
Prepare disk unit . . . . . : 0 % Complete
Start compression (if needed) . . . . . :
Replace status . . . . . :

Number of unreadable pages:

Wait for next display or press F16 for DST main menu

```

Figure 3-41 The Replace Disk Unit Data Status screen

15. Check the configuration by performing the following tasks:
  - a. From the DST main menu, select the option for Work with Disk Units.
  - b. Select the option for Work with Disk Unit Configuration.
  - c. Select the option for Display Disk Unit Status.
  - d. In the Display Disk Configuration Status screen shown in Figure 3-42, check whether the load source (unit 1) is one of the new (larger) disks you require.

Display Disk Configuration Status						
ASP	Unit	Serial Number	Type	Model	Resource Name	Status
1						Mirrored
	1	68-0C82161	6718	050	DD004	Active
	1	68-0C231E9	6718	050	DD005	Resuming
	2	75-0D7B2A2	6718	050	DD003	Active
	2	75-0D7EDB4	6718	050	DD002	Active
Press Enter to continue.						
F3=Exit                  F5=Refresh                  F9=Display disk unit details						
F11=Disk configuration capacity      F12=Cancel						

Figure 3-42 The Display Disk Configuration Status screen

16. Perform an IPL on the system.

### 3.5.4 Load source migration: RAID system

These scenarios are available for load source to migrate on a RAID-protected system:

- ▶ No spare disk slots anywhere in the system
- ▶ Sufficient spare disk slots to start a new RAIDset with the new drives
- ▶ Insufficient spare disk slots to start a new RAIDset with the new drives

#### Load source migrate RAID system: No spare disk slots in the system

If no spare disk slots are available in the system, perform the following tasks:

1. Perform a full system save.
2. Perform an IPL to the DST.
3. Switch off RAID.
4. Follow the basic procedure for nonprotected systems.
5. Restart RAID.
6. Perform an IPL on the system.

#### Load source migrate RAID system: Spare disk slots available

Check the number of RAIDsets under the load source IOA. If more than one, it means that one or more RAIDsets can be physically moved to another IOA but the RAIDset must be kept together as a set under the new IOA.

Follow these steps:

1. Perform a full system save.
2. Power down the system.
3. Move the nonload source disk RAIDset to another IOA. (Ensure that you move all of the disks in the RAIDset and only the disks in that RAIDset).
4. Install the new disks in the vacated slots.
5. Start RAID on the new disks.
6. Perform disk copy from the load source disk to one of the new disks.
7. Add the remaining new disks into the system ASP.
8. Remove the rest of the old load source RAIDset from configuration by using the "Remove disks from configuration" option in the Work with ASP Configuration screen.
9. Power down the system.
10. Physically remove the old load source disk and its RAIDset from the system.
11. Move the new load source disk to the load source position.
12. Perform an IPL on the system.

### **Load source migrate: Insufficient spare disk slots in the system**

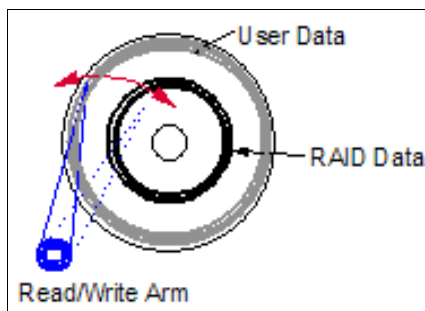
If there are spare disk slots in the system but the numbers are insufficient to allow the installation of a new RAIDset (for example, three or four, depending on the storage IOA):

1. Perform a full system save.
2. Perform an IPL to the DST.
3. Switch off RAID.
4. Install the new drive.
5. Follow the basic procedure described in the earlier section (for unprotected systems).
6. Restart RAID.

## **3.5.5 RAID-5 arrangement on Peripheral Component Interconnect-X I/O adapters**

On January 2003, new PCI-X RAID I/O adapters were announced. These new IOAs support a new form of RAID-5. The new format provides significant performance improvements over the existing PCI RAID IOAs. This also applies to the new i5 servers.

The existing RAID-5 arrangement had the disk platter as one subarray that was split into two sections: the first part of the outer ring of the disk for user data, and the inner ring for RAID data. As seen in Figure 3-43, the Read/Write arm must move across the entire platter even when the disk is partially full. This increases the seek time for data access and consequently the overall response time.



*Figure 3-43 The existing RAID-5 arrangement*

Figure 3-44 shows the new RAID-5 available with the new PCI-X RAID disk IOAs. In this configuration, the disk platter is subdivided into 16 subarrays. Each subarray has a user data area and a RAID data area. You can see that the Read/Write arm only has to move across a fraction of the disk platter at low levels of capacity. This vastly improves the seek time and consequently the response time.

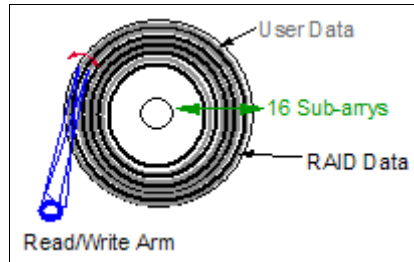


Figure 3-44 RAID-5 arrangement PCI-X RAID IOAs

This new RAID arrangement is implemented by the IOA as soon as any drive under it is started. The major implication of this setup becomes apparent during upgrades. Here are the two scenarios where the new RAID is implemented:

- ▶ When “RAIDed” disks are moved from under the control of an existing PCI RAID IOA to a system unit or expansion unit containing PCI-X RAID Disk IOAs
- ▶ When a new PCI-X RAID Disk IOA replaces an existing PCI RAID Disk IOA controlling “RAIDed” disks in an existing system unit or expansion tower

There is no user control over the change to the RAID arrangement. Because the system runs an IPL for the first time after the new PCI-X IOAs are in place, the IOA detects the old RAID format. During the IPL, the old RAID format is removed and replaced with the new RAID format. During this period, the drives that are being reformatted are not protected. Therefore, ensure that full system backups have been taken.





## System i5 consoles in i5/OS V5R4

This chapter describes the different console types that are available for the System i5 environment: Twinaxial Console, Operations Console (direct), Operations Console (local area network), Hardware Management Console (HMC) 5250, and Thin Console.

This chapter also provides a guide for setting up and maintaining the Thin Console, general information about the console card locations on System i5 servers, and the use of service functions 65+11 to change the console type.

## 4.1 Introduction to the consoles on System i5 servers

This section describes the different types of consoles that are available to manage your System i5 server:

- ▶ Twinaxial console
- ▶ Operations console (direct-attached or LAN-attached)
- ▶ HMC 5250
- ▶ Thin console

### 4.1.1 Twinax console

Originally, only one console type was available, a twinax terminal connected to a twinax card that provided a 5250 console interface to the System i5 server. Although the twinax terminal has been withdrawn from the market, the twinax adapter cards remain available for order on the new 5xx and 5xx+ systems.

The twinax console can still be used on a stand-alone system, or as a console for a system partition. However, it no longer allows for logical partition (LPAR) configuration and management on the new 5xx models. (HMC is a prerequisite for LPAR on any 5xx system.)

### 4.1.2 Operations console (direct-attached or LAN-attached)

An alternative to the twinax console was introduced with the operations console. The first generation could only be directly attached to a serial port. This is referred to as a direct-attached operations console. Later, support was added to connect the PC to a dedicated LAN adapter card. This is commonly known as a LAN console.

The Operations console runs on a PC, as part of the iSeries Access for Windows.™ A green screen console session is provided by the 5250 emulation function of either iSeries Access or IBM Personal Communications. You can also use iSeries Navigator for management functions. Operator panel functions to a nonpartitioned system or to the primary partition are available through a graphical user interface (GUI). The direct-attached Operations console requires an additional special cable.

LAN console allows console sessions to multiple systems or partitions at the same time. More than one PC that is configured as a LAN console can connect to a single system or partition. However, only one can take control of the console session at a given moment.

Both direct-attached and LAN-attached consoles allow incoming dial-in connections to the PC, which facilitates remote access and system management.

### 4.1.3 The Hardware Management Console

This topic describes the virtual console terminal emulation functionality of the HMC. For more information about HMC installation and configuration, system management, remote management (Web-based System Manager (WebSM) and SSH), and Advanced System Management Interface (ASMI), refer to *Logical Partitions on System i5: A Guide to Planning and Configuring LPAR with HMC on System i*, SG24-8000.



## Using the Hardware Management Console as a partition console

With the introduction of the 5xx models, the LPAR configuration and management functions were removed from the iSeries service tools and transferred to the HMC. The HMC performs logical partitioning functions, service functions, and various system management functions. It is a prerequisite to LPAR configuration and Capacity on Demand in any System i5 environment.

The HMC connects to the managed system through an Ethernet LAN connection to port HMC1 or HMC2 of the Service Processor (SP) in the CEC. A virtual console terminal can be configured to run on the HMC for each partition, thus reducing the requirement for extra hardware in each partition. One of these console types is 5250.

Configure the 5250 partition consoles on System i5 servers in the following ways:

- ▶ Use only the HMC as the partition console.
- ▶ Use the HMC as the partition console, and define a twinax console device or operations console device as an alternate console device for a partition.
- ▶ Not use the HMC as a partition console, and specify a twinax console or operations console as the partition console.

When you use the HMC as the partition console, connect to the 5250 console locally or remotely.

### ***Connecting to the 5250 console locally***

To open a console session in the HMC, perform the following tasks:

1. In the navigation area, select the managed system and select **Server and Partition** → **Server Management**.
2. The Server and Partition: Server Management pane is displayed. Expand the Partitions folder, select the desired partition, and right-click. This gives you the option to open either a dedicated 5250 console or a shared 5250 console.

If you open a shared 5250 console, another user can open a 5250 emulation window and share the session with you. Because this is really one session being shared between users, there is no control switching mechanism. Everything you type in the shared session is visible to the other user.

### ***Connecting to the 5250 console remotely***

If your HMC is located in the machine room, the use of the HMC as the partition console means that you have to go over to the machine room whenever you require a console session. To circumvent this and facilitate system management, you can use the remote connection functionality that is available through the following emulators:

- ▶ IBM iSeries Access PC5250 emulator, V5, R3 with PTF SI13587 or later
- ▶ IBM Personal Communications 5250 emulator, V5.7 or later
- ▶ iSeries Access for Linux emulator, V5.2.0-1.4 or later

The HMC user ID and password are required to connect to the console session. For configuration instructions and information about remote security and the HMC firewall, refer to the topic *System i: Managing the HMC 5250 console* from the IBM Systems Hardware Information Center, which is available on the Web at:

<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/topic/iphb8/iphb8.pdf>

## HMC and server firmware code-level update

Your HMC is a critical part of your hardware configuration. It is recommended that you keep both the server firmware level and the HMC machine code up to date.

### ***Server firmware (Licensed Internal Code)***

The server firmware is the part of the Licensed Internal Code (LIC) that enables hardware. It is stored in the Service Processor. The Service Processor stores a permanent copy (“p” side) and a temporary copy (“t” side). It is recommended that you run the managed server from the “t” side.

The firmware level is displayed as SFXXX\_YYY, where XXX is the release level, and YYY is the fix level. Firmware fixes are displayed as MHnnnnn.

When you upgrade to a new release, the process is always disruptive; that is, the managed system and not just the partitions have to be shut down and restarted in order to accept the new release level. The fix updates within the same release *can be*, but are not always concurrent. It is recommended that after you have started an update or upgrade process, you do not interrupt it or perform any other tasks.

For details about the update or upgrade process, refer to the topic “obtaining firmware updates” in the IBM Systems Hardware Information Center, which is available on the Web at: [http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/topic/ipha5/fix\\_serv\\_firm\\_kick.htm](http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/topic/ipha5/fix_serv_firm_kick.htm)

**Note:** The HMC machine code must be equal to or greater than the server firmware level. The sequence in which you install fixes or updates is very important. Install the HMC updates *before* you install the server firmware updates in order to ensure that the HMC machine code can handle the server firmware level that you are applying. See “Supported combinations of server firmware and HMC code” on page 96.

You can use either the HMC to manage, download, and install your firmware level and fixes (which is the default setting) or the program temporary fix (PTF) functions of the i5/OS. These options are referred to as “Update policy set to HMC” versus “Update policy set to operating system”.

If you decide to set the update policy to the operating system, you must define one of your logical partitions as the *service partition*. After changing the update policy, the next IPL of the service partition will cause the server firmware level on the managed system to be flashed with the current level of the server firmware portion of the LIC on the service partition. This process is known as LS Flash Synching (Firmware Load Source to SP Flash synchronization).

Therefore, it is important that you check the current level of firmware on the service partition before you make the change, and ensure that it is at the same level or at a higher level than the server firmware running on the managed system. Also consider the consequences in the event of a scratch install of the service partition. To avoid these situations, it is recommended that you set the update policy to HMC instead of operating system.

The only situation where you will be forced to change the update policy from HMC to operating system and designate a service partition is when you go from a system that was previously managed by an HMC to a system that is no longer managed by an HMC. You will receive the following error message to signal this situation:

“This partition does not have the authority to perform the requested function. Verify that this partition has service authority. If the problem persists after granting the partition service authority, then contact your service support structure.”

Refer to the following sites to download server firmware fixes:

- ▶ iSeries Recommended Fixes - Server Firmware: Update Policy Set to Operating System  
[http://www-912.ibm.com/s\\_dir/slkbase.nsf/c32447c09fb9a1f186256a6c00504227/604992740f846a4986256fd3006029b5?OpenDocument](http://www-912.ibm.com/s_dir/slkbase.nsf/c32447c09fb9a1f186256a6c00504227/604992740f846a4986256fd3006029b5?OpenDocument)
- ▶ iSeries Recommended Fixes - Server Firmware: Update Policy Set to HMC  
[http://www-912.ibm.com/s\\_dir/slkbase.nsf/ibmscdirect/E58D7BBF0EAC9A2786256EAD005F54D8](http://www-912.ibm.com/s_dir/slkbase.nsf/ibmscdirect/E58D7BBF0EAC9A2786256EAD005F54D8)

### **HMC machine code**

An overview of the supported HMC machine code levels is available at:

<https://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html>

Figure 4-1 shows the HMC machine code levels.

## Hardware Management Console

Support for UNIX servers and Midrange servers

### HMC corrective service support

These pages deliver corrective service and other download support for the Hardware Management Console (HMC) for both POWER5™ and POWER4™ servers. Online media ordering, installation instructions and related technical information are also provided.

Your IBM support center provides technical support for the HMC.

### HMC products for servers with POWER5 processors

Version	Releases
HMC Version 6	HMC 6.1
HMC Version 5	HMC 5.2.1      HMC 5.2      HMC 5.1
HMC Version 4	HMC 4.5      Older versions

### HMC products for servers with POWER4 processors

Version	Releases
HMC Version 3.3	HMC 3.3.7 and lower releases
HMC Version 3.2 LPP-based	HMC 3.2 and lower versions

**Note:** HMC 3.2.x and lower are lpp-based versions of the HMC code. These versions support POWER4 servers (IBM eServer pSeries). To upgrade to the machine code version, your lpp-based HMC must first be upgraded to HMC 3.2.6, the highest-level release of the lpp-based code.

**End-of-Service Reminder:** HMC 3.2 and lower products are no longer supported, effective August 31, 2006.

### BIOS updates

This site provides BIOS updates only for those HMC models (PCs) that require a BIOS update for the HMC to work correctly. BIOS updates are not provided for HMC models that do not require updates for HMC functionality.

→ [BIOS updates for the HMC](#)

### Additional resources

- [POWER5 code matrix](#)
- [HMC best practices](#)
- [i5, iSeries support](#)
- [UNIX servers support](#)
- [Microcode downloads System i and System p](#)

Sign up for email notification of HMC corrective service.

- [System p](#)
- [System i](#)

Figure 4-1 HMC machine code levels

Select the release level, and download either the fixes for that release (corrective service download) or get a release update (recovery media download). Installation instructions are also available. Here is an example for HMC machine code 5.2.1:

- ▶ Corrective service download (Figure 4-2), which is available at:  
<https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power5/download/v521.Update.html>

**Hardware Management Console**  
Support for HMC 5.2.1 for UNIX servers and Midrange servers

**Corrective service** | Recovery media | HPSNM/IBMNM fixes

**Downloads** | Installation instructions | Related documentation

↓ Download multiple files    ↓ Download individual files or order CDs

Download the HMC 5.2.1 update/upgrade package and fixes for HMC 5.2.1 from this page.

**Upgrade notes**

**Upgrading HMC V4 to HMC 5.x**

There is no Corrective Service to update to HMC Version 5 from Version 4. You must perform an Upgrade via Recovery media to update from HMC 4 to any HMC Version 5.x. Before upgrading, you must use the Save Upgrade Data task to preserve existing configuration on the HMC, such as partition profiles and HMC configuration.

**Upgrading to HMC 5.2.1**

You can upgrade to HMC V5R2.1 in the following manners:

- If you are currently at HMC V5R2.0, you can use the Update images (PTF MH00594) to update your HMC to V5R2.1. After the update, the output from the **lshmc -V** command will show a **base\_version** string of **V5R2.0**. You do not need to apply PTF MH00653 if you are already using the update images from MH00594 to update your HMC to V5R2.1.
- If you are currently at HMC V4R1.1 through HMC V5R1.0, you must use the [Recovery media](#) (PTF MH00653) to upgrade your HMC to V5R2.1. After the upgrade, the output from the **lshmc -V** command will show a **base\_version** string of **V5R2.1**.

HMC V5R2.1 contains fixes from MH00586 and MH00610

**Download multiple files via Download Director**

Download multiple ZIP or ISO image files simultaneously by choosing an option from the drop-down menu on the following selection box.

Select a package to download

The **View** links in the [individual downloads table](#) provide important information used to verify corrective

**Other releases**  
[Select another HMC Release.](#)

**Additional resources**

- [i5, iSeries support](#)
- [UNIX servers support](#)
- [Microcode downloads for i5, iSeries, p5, pSeries](#)

[Sign up for email notification of HMC corrective service.](#)

Figure 4-2 HMC corrective service downloads

- ▶ Recovery media download (Figure 4-3 on page 95)  
<https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power5/download/v521.Recovery.html>

The *HMC Recovery DVD*, which is used to update your code to a new release, is a bootable image and contains the HMC Base Code. If you have to scratch install the HMC machine code, you require the recovery DVD for the release installed on the HMC. Before you start an upgrade, ensure that you have performed the following tasks:

- Back up the managed system's profile data.

- Back up the critical console information (this enables you to go back to the previous level of machine code in case something goes wrong when upgrading).
- Record HMC configuration information (schedule operations) and remote command status.
- Save the upgrade data.

Upgrade data enables you to restore the HMC configuration after the upgrade. The upgrade data is stored in a designated disk partition on the HMC. Only one version of the upgrade data can be stored at a time, so perform this operation immediately before the upgrade.

For details about the upgrade process, refer to:

[http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/topic/ipha5/fixeshmc\\_upgrades.htm](http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/topic/ipha5/fixeshmc_upgrades.htm)

## Hardware Management Console

Support for HMC 5.2 on UNIX servers and Midrange servers

[Corrective service](#)
[Recovery media](#)
[HPSNM/IBMNM fixes](#)

[Downloads](#)
[Installation instructions](#)
[Related documentation](#)

[Other releases](#)

Select another HMC Release.

[Additional resources](#)

- POWER5 code matrix
- i5, iSeries support
- UNIX servers support
- Microcode downloads for i5, iSeries, p5, pSeries

[Sign up for email notification of HMC corrective service.](#)

↓ [Obtaining the HMC 5.2.1 Recovery media](#)

The HMC 5.2.1 Recovery media package (PTF MH00653) is equivalent to the HMC 5.2.1 Update package (PTF MH00594) except that it represents Recovery DVDs for HMC 5.2.1. The Recovery DVDs provide a new BIOS used in 7310CR3 RoHS-compliant machines. The BIOS is installed during Recovery DVD installation/upgrade process.

### Upgrade notes

#### Upgrading HMC V4 to HMC 5.x

There is no Corrective Service to update to HMC Version 5 from Version 4. You must perform an Upgrade via Recovery media to update from HMC 4 to any HMC Version 5.x. Before upgrading, you must use the Save Upgrade Data task to preserve existing configuration on the HMC, such as partition profiles and HMC configuration.

#### Upgrading to HMC 5.2.1

You can upgrade to HMC V5R2.1 in the following manners:

- If you are currently at HMC V5R2.0, you can use the [Update images](#) (PTF MH00594) to update your HMC to V5R2.1. After the update, the output from the **lshmc -V** command will show a **base\_version** string of **V5R2.0**. You do not need to apply PTF MH00653 if you are already using the update images from MH00594 to update your HMC to V5R2.1.
- If you are currently at HMC V4R1.1 through HMC V5R1.0, you must use the Recovery media (PTF MH00653) to upgrade your HMC to V5R2.1. After the upgrade, the output from the **lshmc -V** command will show a **base\_version** string of **V5R2.1**.

HMC V5R2.1 contains fixes from MH00586 and MH00610

### Obtaining the HMC 5.2.1 Recovery media

The HMC Recovery DVD V5 R2.1 is a bootable image. You can order DVD media from this page or download the DVD images in ISO format, which you can then use to burn your own DVDs. See the "Installation instructions" for procedures and downloads for installation over a network.

- ↓ [Download ISO images via Download Director](#)
- ↓ [Download ISO images individually](#)
- ↓ [Order recovery media](#)

Figure 4-3 HMC Recovery DVD download

## Supported combinations of server firmware and HMC code

Figure 4-4 shows the supported combinations of server firmware and HMC code.

**Note:** The HMC machine code must be equal to or greater than the server firmware level. The sequence in which you install fixes or updates is important. Install the HMC updates before you install the server firmware updates to ensure that the HMC machine code can handle the server firmware level that you are applying,

HMC levels	POWER 5 system firmware levels (iSeries and pSeries)						
	240 Release	235 Release	230 Release	225 Release	222 Release	220 Release	210 Release
<b>HMC V5R2</b> Minimum HMC Level Required to Support POWER5 Release Level 240	Supported HMC and system firmware combination.	Supported HMC and system firmware combination. FW Release covered under general FW support thru 10/2006	Supported HMC and system firmware combination. FW Release covered under general FW support thru 12/2006.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.
<b>HMC V5R1</b> Minimum HMC Level Required to Support POWER5 Release Level 235	Not a supported combination.	Recommended and supported HMC and system firmware combination. FW Release covered under general FW support thru 10/2006	Supported HMC and system firmware combination. FW Release covered under general FW support thru 12/2006.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.
<b>HMC V4R5</b> Minimum HMC Level Required to Support POWER5 Release Level 230	Not a supported combination.	Not a supported combination.	Recommended and supported HMC and system firmware combination. FW Release covered under general FW support thru 12/2006.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.
<b>HMC V4R4</b> Minimum HMC Level Required to Support POWER5 Release Level 225	Not a supported combination.	Not a supported combination.	Not a supported combination.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.
<b>HMC V4R3</b> Minimum HMC Level Required to Support POWER5 Release Level 222	Not a supported combination.	Not a supported combination.	Not a supported combination.	Not a supported combination.	Service Packs no longer provided.	Service Packs no longer provided.	Service Packs no longer provided.
<b>HMC V4R2</b> Minimum HMC Level Required to Support POWER5 Release Level 220	Not a supported combination.	Not a supported combination.	Not a supported combination.	Not a supported combination.	Not a supported combination.	Service Packs no longer provided.	Service Packs no longer provided.
<b>HMC V4R1</b> Minimum HMC Level Required to Support POWER5 Release Level 210	Not a supported combination.	Not a supported combination.	Not a supported combination.	Not a supported combination.	Not a supported combination.	Not a supported combination.	Service Packs no longer provided.
Matrix Key: <b>Latest Release Level</b>   <b>Maximum Stability Release Level</b>   <i>Reduced Fix support</i>   <b>End of Service Pack support</b> Service Packs no longer provided. IBM recommends updating your firmware and HMC to a recommended Release Level.							

Figure 4-4 Supported combinations of server firmware and HMC code

Check for updated information about the supported combinations server firmware and the HMC code levels at the POWER5 code matrix Web site:

<http://www14.software.ibm.com/webapp/set2/sas/f/power5cm/supportedcode.html>

For more information about getting and installing fixes and updates for HMC code and server firmware, refer to the IBM Systems Hardware Information Center or download the PDF at:

<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/topic/iph5/iph5.pdf>

Receive updates on the latest fix levels through the subscription service for System i5 at:

<http://www14.software.ibm.com/webapp/set2/subscriptions/iqvcmjcd>



## 4.2 Thin Console

Thin Console is a new type of console. It is available only for selected *nonpartitioned* System i5, 9405-520, 9406-520, and 9406-550. These models must be running i5/OS V5R3 or later and a firmware level of SF240 or later.

The Thin Console was designed to deliver a low-cost and easy-setup alternative for console function on nonpartitioned systems that do not require an HMC. It provides a 5250 console session to the system. The cable connects directly from the device Ethernet port to the SP's HMC1 or HMC2 Ethernet port on the server, thus not taking any IOA/IOP (input/output adapter/input/output processor) slot. The console type is displayed as HMC to the i5/OS. Coexistence of a Thin Console and an HMC is *not* supported.

The Thin Console is a Neoware c50 thin client running a customized Linux image, which includes an IBM 5250 emulator. It boots from internal flash memory. To update the code or reinstall the Linux image, download the Linux image from the Web as a .zip file and extract it to a Universal Serial Bus (USB) memory stick. Because the image does not take up much space, the minimum requirement for the memory stick is only 128 MB.

You cannot install separate fixes to the code. Any update must be performed by overwriting the entire Linux image with the new one.

When you order a system with a Thin Console, it does not automatically include a display. Therefore, either add it to your order or provide one yourself.

Figure 4-5 shows a System i5 Thin Console.



Figure 4-5 System i5 Thin Console

### 4.2.1 Thin Console installation

The Thin Console is supported only on selected *nonpartitioned* System i5, 9405-520, 9406-520, and 9406-550. These models must be running i5/OS V5R3 or later and a firmware level of SF240 or later.

### 4.2.2 Specifications

The Thin Console is a Neoware c50 thin client running a customized Linux image, which includes an IBM 5250 emulator.

The Linux software image does *not* include support for printing or for programmable or scriptable interfaces (application programming interfaces (APIs), commands, and scripts).

The Neoware c50 thin client contains:

- ▶ 1 VIA Eden Processor @ 400 MHz
- ▶ 64 MB of flash storage
- ▶ 128 MB of DDR SDRAM memory
- ▶ 1 serial port (D-Sub 9-Pin Male)
- ▶ 1 parallel port (D-Sub 25-Pin Female)
- ▶ 1 VGA port, with support for up to 1200x1600 @ 60 Hz
- ▶ 1 PS/2 keyboard port
- ▶ 1 PS/2 mouse port
- ▶ 2 USB 2.0 ports (type A)

The documentation for the Neoware c50 thin clients with their generic NeoLinux 3.0 load, *NeoLinux Thin Clients User Manual*, is available at:

- ▶ [http://www.neoware.com/docs/manuals/um\\_neolinux\\_30\\_20040630.pdf](http://www.neoware.com/docs/manuals/um_neolinux_30_20040630.pdf)

The Thin Console has two interactive user interfaces:

- ▶ A 5250 screen
  - When connecting to the server, it displays the connection status.
  - After successful connection, it displays the server's 5250 console session.
- ▶ A GUI-type configuration screen for the keyboard and monitor called the ezConnect - Neoware Connection Manager

### 4.2.3 Thin Console 5250 emulation screen

Figure 4-6 on page 99 shows the connection status screen, which displays console information, server information, and connection status.



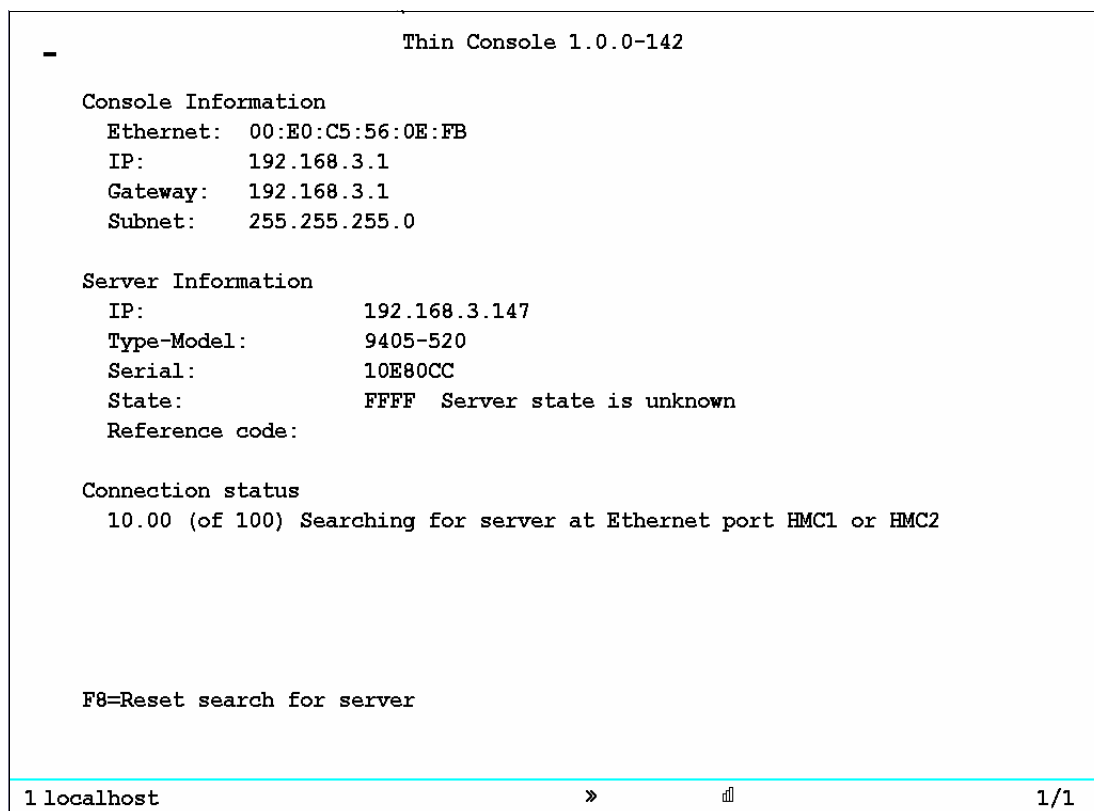


Figure 4-6 Thin console connection status screen

Under Server Information, the State field indicates the power and runtime states as they are detected by the Thin Console. The State field contains a numeric status code and a description. Table 4-1 lists the codes and their meanings.

Table 4-1 Server information state codes

Numeric code	Code names	Description
0x00	CEC_NOT_RUNNING	"POWERED OFF"
0x01	CEC_IPLING_PHY_P_NOT_READY_FOR_HMC	"STARTING"
0x02	CEC_IPLING_PHY_P_READY_FOR_HMC	"STARTING"
0x03	CEC_TERMINATION	"TERMINATING"
0x04	CEC_DUMPING	"FIRMWARE DUMP"
0x05	CEC_POWER_ON_TRANSITION	"STARTING"
0x06	CEC_POWER_OFF_TRANSITION	"POWERING OFF"
0x07	CEC_POWER_OFF_IN_PROCESS	"POWERING OFF"
0x08	CEC_TRANSITION_TO_IPL	"STARTING"
0x09	CEC_TRANSITION_TO_DUMP	"FIRMWARE DUMP"
0x0A	CEC_TRANSITION_TO_TERMINATION	"TERMINATING"
0x0F	CEC_PHY_P_FUNCTIONAL	"FIRMWARE READY"

0xFFFF	CEC_RUN_STATE_UNKNOWN	"UNKNOWN"
Any other state	n/a	"UNKNOWN"

Under Connection Status, the server connection status code indicates the progress of the connection between the Thin Console and the server. It is a four-digit code XX.YY, where XX is the major connection status (00-99) and YY is the minor connection status (00-99).

Table 4-2 lists the status codes and their description. During a successful connection, these codes must progress from 0 to 100.

*Table 4-2 Server connection status codes*

<b>Numeric code</b>	<b>Code names</b>	<b>Description</b>
00	NO_CONNECTION	"SEARCHING FOR SERVICE PROCESSOR"
10	CONNECTION_TO_HWS	"SEARCHING FOR SERVICE PROCESSOR"
20	CMD_SOCKET_UP	"SERVICE PROCESSOR FOUND"
30	STREAM_SOCKET_UP	"VALIDATING SYSTEM POWER™ STATE"
40	PHYP_UP	"FIRMWARE READY"
50	SERIAL_CONNECTION_UP	"COMMUNICATION INITIALIZED"
60	LINK_LEVEL_ECHO_UP	"COMMUNICATION ACTIVE"
70	ICMP_ECHO_POLLING_UP	"IP COMMUNICATION ACTIVE"
80	HWS_IS_ECHOING	"IP COMMUNICATION ACTIVE"
90	GOT_INIT_COND_RESPONSE	"OPERATING SYSTEM CONSOLE INITIALIZED"
93	CONNECTED_TO_SLIC	"OPERATING SYSTEM CONSOLE ACTIVE"
97	NEGOTIATING	"NEGOTIATING"
99	WAITING_FOR_SCREEN	"WAITING FOR SCREEN DATA"
100	PASS_DATA_THROUGH	The user should see the i5/OS 5250 data stream when at this state.

## 4.2.4 Neoware Connection Manager

Figure 4-7 shows the GUI screen for the configuration of the keyboard and the monitor. Use Ctrl+Alt+End to switch from the 5250 screen to the configuration screen. To go back to the 5250 screen, double-click the **5250 Console** connection.

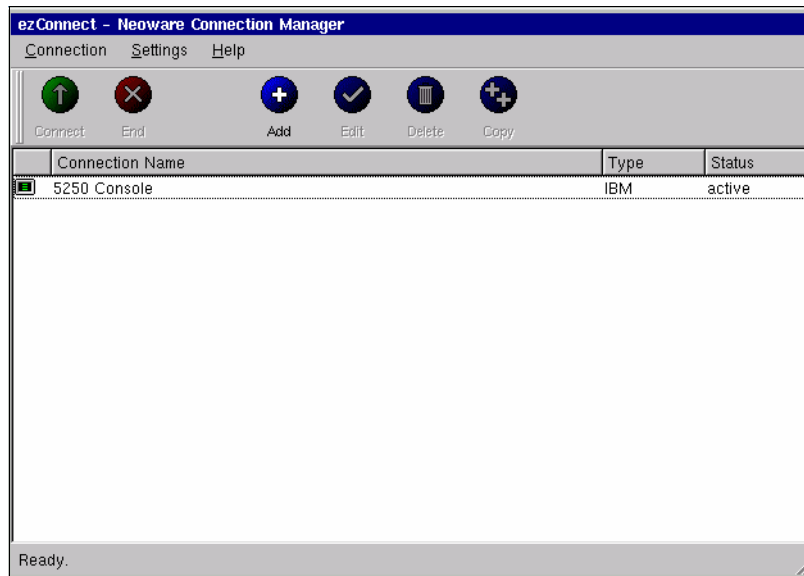


Figure 4-7 GUI configuration screen

## 4.2.5 Physical installation and cabling

On the System i5 server side, you do not have to install any hardware. The Thin Console connects directly to one of the HMC ports of the Service Processor (SP), instead of connecting to an IOA card. Perform the following tasks to install the Thin Console:

1. Verify the hardware that came with your order. It must contain the Neoware c50 thin client, a keyboard, a mouse, and a power cable (and optionally, a display).
2. Connect the display, keyboard, mouse, power cable, and Ethernet cable to the ports on the Thin Console (Figure 4-8).

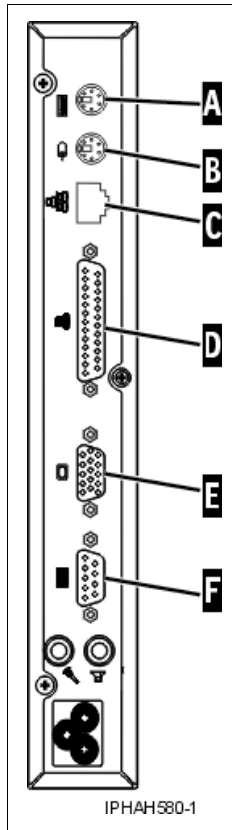


Figure 4-8 Thin Console back view

3. Plug in the monitor and power it on.
4. Plug in the Thin Console. It automatically powers on. It boots from the pre-installed Linux software image; you do not have to install any software.
5. Select the keyboard language and press Enter (Figure 4-9 on page 103).

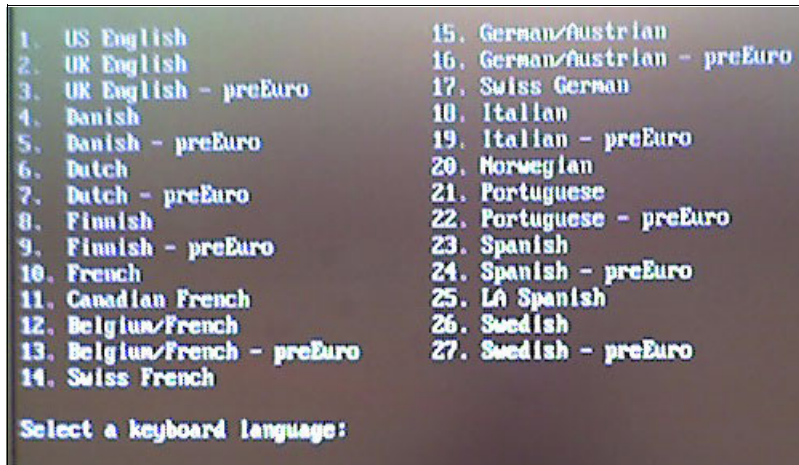


Figure 4-9 Thin Console: Select a keyboard

6. Plug the other end of the Ethernet cable directly into either one of the HMC ports on the server. The ports are labeled HMC1 and HMC2. Although it is recommended that you attach the Thin Console before powering on the server, the console session must be able to connect regardless of the connection sequence.

**Note:** Do not attach another console device to the remaining HMC port. When you use a Thin Console, only one HMC port on the FSP can be connected at a time.

7. The 5250 session comes up and displays the progress of the connection status. Figure 4-10 shows connection status 10.nn.

```

-                               Thin Console 1.0.0-142

Console Information
  Ethernet:  00:E0:C5:56:0E:FB
  IP:        192.168.3.1
  Gateway:   192.168.3.1
  Subnet:    255.255.255.0

Server Information
  IP:        192.168.3.147
  Type-Model: 9405-520
  Serial:     10E80CC
  State:      FFFF Server state is unknown
  Reference code:

Connection status
  10.00 (of 100) Searching for server at Ethernet port HMC1 or HMC2

F8=Reset search for server

```

Figure 4-10 Thin Console connection status 10.nn

8. On the next screen (Figure 4-11), authenticate the device to the FSP by entering the HMC access password. The default password is abc123. This authentication ensures protection for the FSP network interfaces. After being entered, the access password is stored locally on the Thin Console, so that subsequent connections to the same FSP do not require you to re-enter it.

```
Thin Console 1.0.0-142

Console Information
Ethernet: 00:E0:C5:56:0E:FB
IP:      192.168.3.1
Gateway: 192.168.3.1
Subnet:  255.255.255.0

Server Information
IP:      192.168.3.147
Type-Model: 9405-520
Serial:    10E80CC
State:     FFFF Server state is unknown
Reference code:

Connection status
10.01 (of 100) Searching for server at Ethernet port HMC1 or HMC2

1 - Enter HMC access password:
-

F8=Reset search for server
```

Figure 4-11 Thin Console connection status: Authentication

9. If you have not done so already, power on the System i5. The following figures (Figure 4-12, Figure 4-13 on page 105, and Figure 4-14 on page 105) show the Thin Console cycling through some of the different connection states.

Figure 4-12 shows the Thin Console connection status 20.nn.

```
Server Information
IP:      192.168.3.147
Type-Model: 9405-520
Serial:    10E80CC
State:     FFFF Server state is unknown
Reference code:

Connection status
20.00 (of 100) Server found
```

Figure 4-12 Thin Console connection status 20.nn

Figure 4-13 shows Thin Console connection status 40.nn.

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:              000F  Server firmware ready
Reference code:

Connection status
40.01 (of 100) Server firmware is ready to communicate
```

Figure 4-13 Thin Console connection status 40.nn

Figure 4-14 shows Thin Console connection status 60.nn.

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:              000F  Server firmware ready
Reference code:

Connection status
60.01 (of 100) Requesting console access
```

Figure 4-14 Thin Console connection status 60.nn

10. When the connection to the server is completed, the Thin Console 5250 session behaves like any other 5250 console (Figure 4-15).

```
                Dedicated Service Tools (DST) Sign On
                                           System:  S10E80CC

ATTENTION:  This device can become the console.

Type choices, press Enter.

Service tools user . . . . . _____
Service tools password . . . . . _____
```

Figure 4-15 DST Sign On screen

11. When you power down the system (or IPL), the FSP port remains powered on. Because the Thin Console is directly connected to the FSP, it is able to detect that connection, even when the i5/OS system is not running. In such a situation, the system attention light is on. It will go off as soon as the server powers on. The following figures (Figure 4-16 to Figure 4-26 on page 109) show the codes displayed by the Thin Console to signal this. Note the Server Information State, Server Information Reference Code, and Connection status fields.

Figure 4-16 shows power off 10.00.

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             FFFF  Server state is unknown
Reference code:

Connection status
10.00 (of 100) Searching for server at Ethernet port HMC1 or HMC2
```

Figure 4-16 Power off 10.00

Figure 4-17 shows power off 20.00.

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             0000  Server powered off
Reference code:

Connection status
20.00 (of 100) Server found
```

Figure 4-17 Power off 20.00

Figure 4-18 through Figure 4-21 on page 107 show four stages of power off 30.00.

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             0000  Server powered off
Reference code:

Connection status
30.00 (of 100) Waiting for server to power on
```

Figure 4-18 Power off 30.00 1 of 4



```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             0000  Server powered off
Reference code:     C1112000

Connection status
30.00 (of 100) Waiting for server to power on
```

Figure 4-19 Power off 30.00 2 of 4

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             0005  Server powering on
Reference code:     C100C1FF

Connection status
30.00 (of 100) Waiting for server to power on
```

Figure 4-20 Power off 30.00 3 of 4

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             0001  Server powering on
Reference code:     C700406E

Connection status
30.00 (of 100) Waiting for server to power on
```

Figure 4-21 Power on 30.00 4 of 4

Figure 4-22 shows power on 40.01.

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             000F  Server firmware ready
Reference code:

Connection status
40.01 (of 100) Server firmware is ready to communicate
```

Figure 4-22 Power on 40.01

Figure 4-23 shows power on 50.00.

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             000F  Server firmware ready
Reference code:     C2003150

Connection status
50.00 (of 100) Searching for operating system
```

Figure 4-23 Power on 50.00

Figure 4-24 shows power on 60.01.

```
Server Information
IP:                192.168.3.147
Type-Model:        9405-520
Serial:            10E80CC
State:             000F  Server firmware ready
Reference code:     C6004027

Connection status
60.01 (of 100) Requesting console access
```

Figure 4-24 Power on 60.01

Figure 4-25 shows that power on is ready.

```
                                IPL or Install the System
                                System:  S10E80CC

Select one of the following:

    1. Perform an IPL
    2. Install the operating system
    3. Use Dedicated Service Tools (DST)
    4. Perform automatic installation of the operating system
    5. Save Licensed Internal Code

Selection
-

Licensed Internal Code - Property of IBM 5722-999 Licensed
Internal Code (c) Copyright IBM Corp. 1980, 2006. All
rights reserved. US Government Users Restricted Rights -
Use duplication or disclosure restricted by GSA ADP schedule
Contract with IBM Corp.
```

Figure 4-25 Power on ready

Figure 4-26 shows the power on IPL steps.

```
-
-          Licensed Internal Code IPL in Progress                                08/18/06  14:11:57

IPL:
  Type . . . . . : Unattended
  Start date and time . . . . . : 08/18/06  14:11:24
  Previous system end . . . . . : Abnormal
  Current step / total . . . . . :    16    16
  Reference code detail . . . . . : C6004065

IPL step                                Time Elapsed   Time Remaining
Commit Recovery                          00:00:01       00:00:00
Data Base Initialization                 00:00:01       00:00:00
Journal IPL Clean up                     00:00:01       00:00:00
Commit Initialization                     00:00:01       00:00:00
>Start the operating system

Item:
  Current / Total . . . . . :

Sub Item:
  Identifier . . . . . :
  Current / Total . . . . . :
```

Figure 4-26 Power on IPL steps

## 4.2.6 Customization settings

From the 5250 session, select Ctrl+Alt+End to go to the ezConnect - Neoware Connection Manager window (Figure 4-27). This GUI enables you to change some of the settings of your Thin Console. This section describes the menu options.

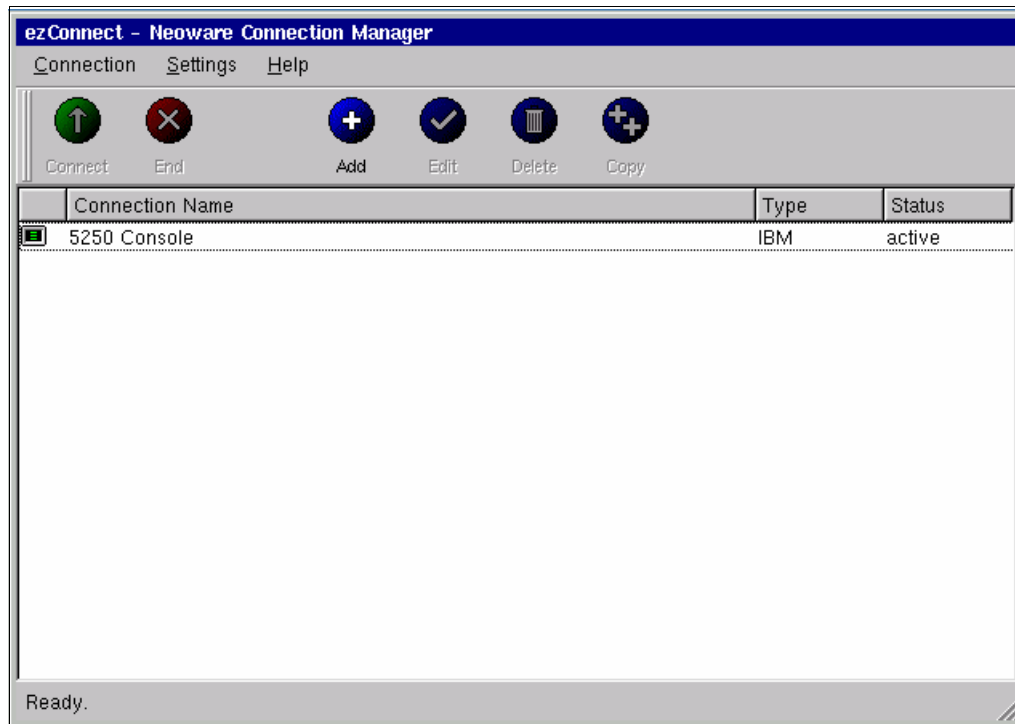


Figure 4-27 Neoware Connection Manager

### Connection menu

Figure 4-28 shows the options that are available from the Connection menu. The Session option enables you to restart the 5250 console connection. If you change any of the connection settings, you have to restart the connection for the changes to take effect.

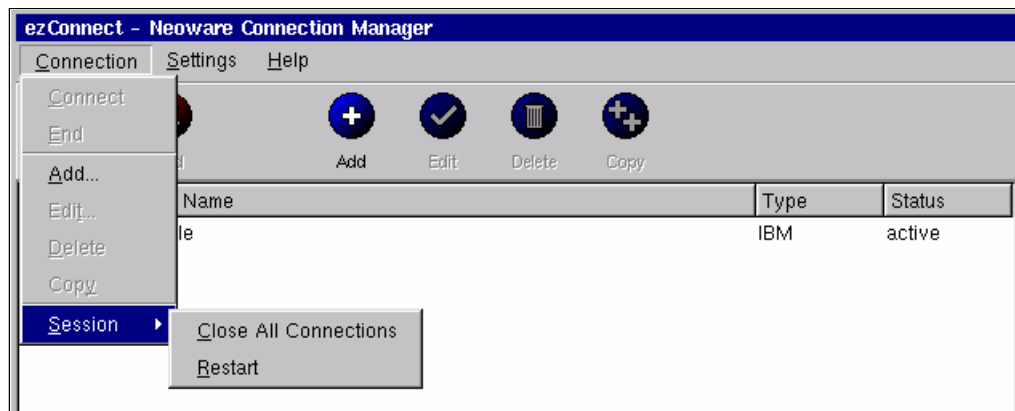


Figure 4-28 Neoware Connection Manager: Connection menu

### Settings menu: Appliance properties

The Appliance properties option (Figure 4-29 on page 111) from the Settings menu enables you to customize some of the Thin Console properties. The options from Network to Desktop

(within a red frame in Figure 4-29) are the general settings. Click **Network** if you want to modify the network settings.

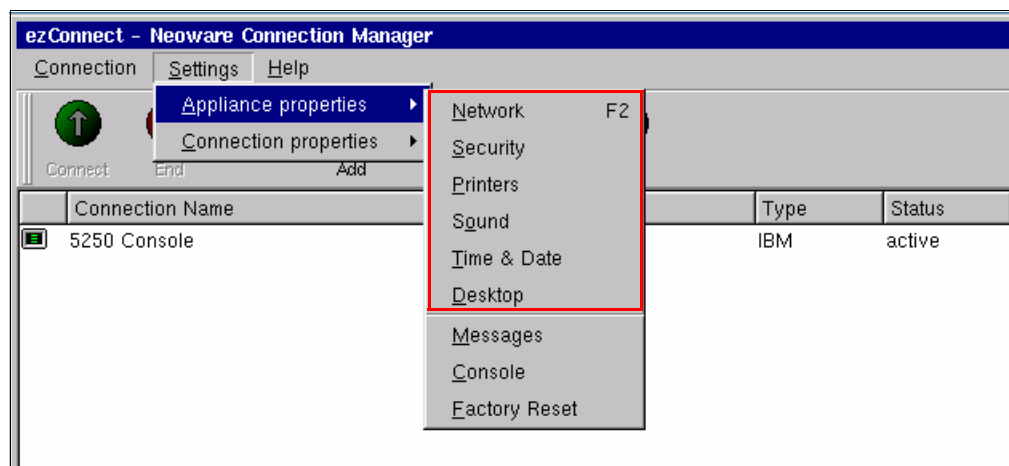


Figure 4-29 Neoware Connection Manager: General settings

Figure 4-30 shows the Network Settings window.

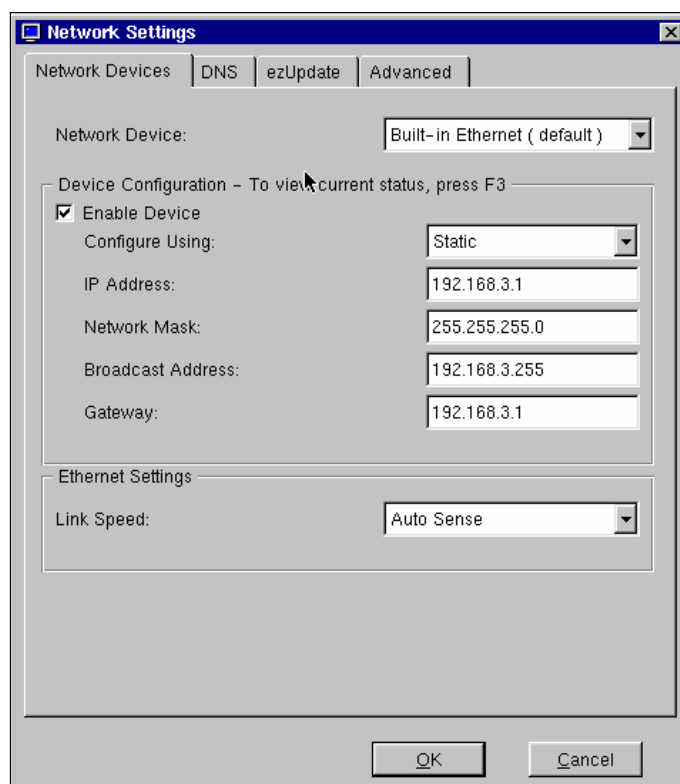


Figure 4-30 Neoware Connection Manager: Network settings

The three other options in the red frame in the Appliance properties (Figure 4-31) are advanced settings. Factory Reset resets the customization to the factory default, and the Console option opens the Appliance Console.

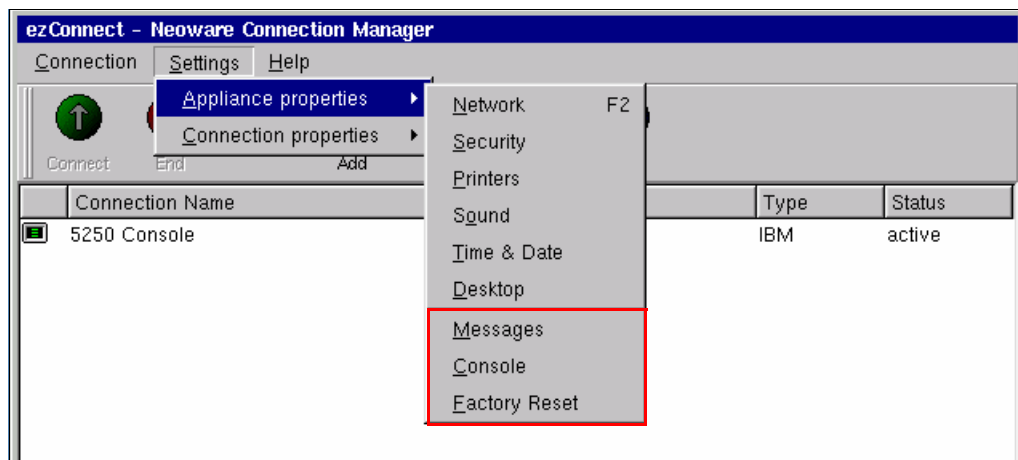


Figure 4-31 Neoware Connection Manager: Advanced settings

In the Appliance Console screen (Figure 4-32), type `menu` and press Enter.

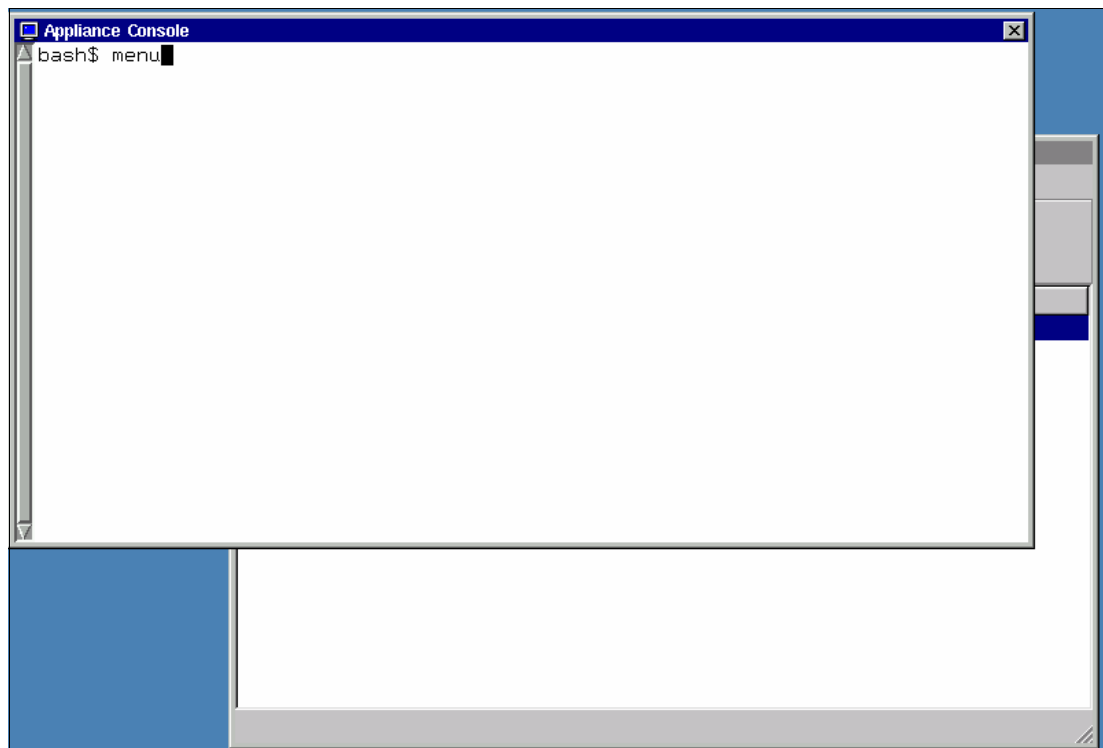


Figure 4-32 Appliance Console

This opens an advanced configuration menu (Figure 4-33). The options in this menu exist to enable problem determination by IBM support personnel. Option 10 overrides the FSP address and stops the automatic network search code.

**Important:** It is recommended that you do not make any changes here.

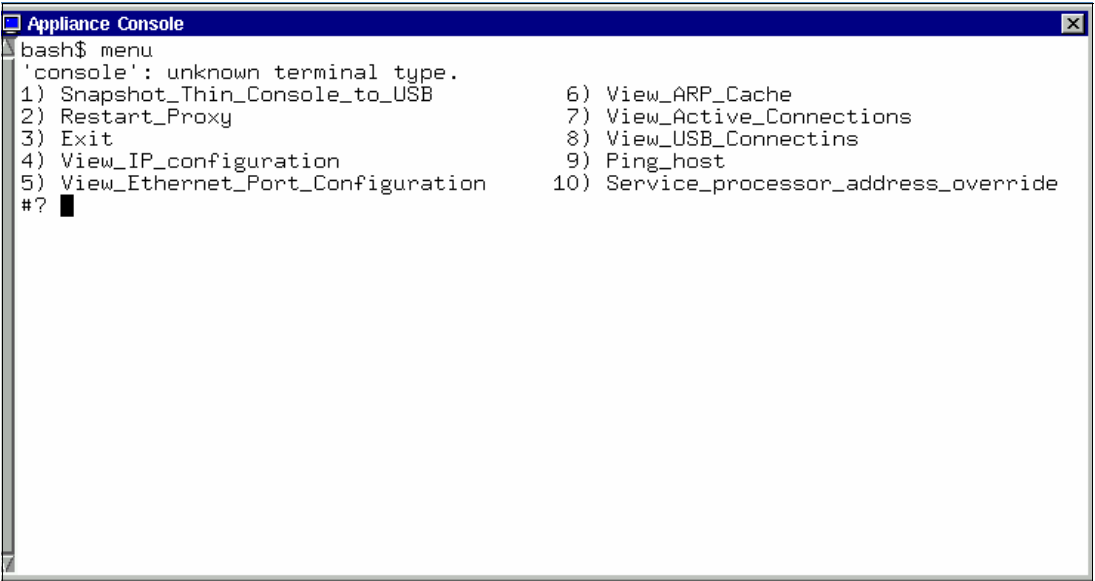


Figure 4-33 Appliance Console: Menu screen

**Settings menu: Connection properties**

To change the terminal settings, select **Settings** → **Connection properties** → **Global IBM Terminal Settings** (Figure 4-34).

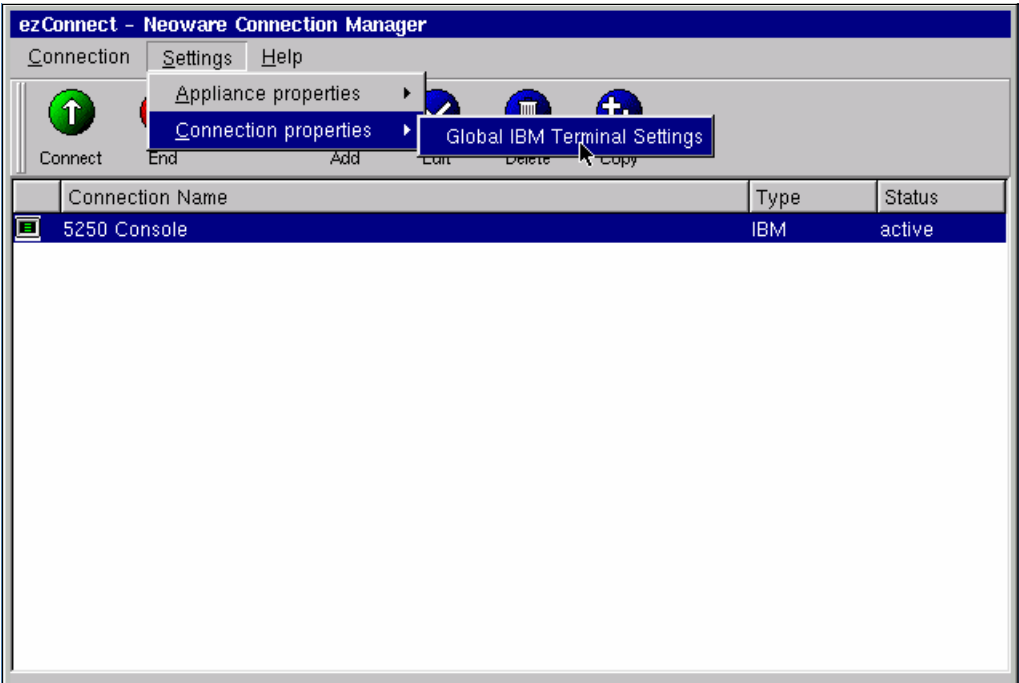


Figure 4-34 Neoware Connection Manager: Global IBM Terminal Settings

An example of customization is the color mapping for the 5250 session. Perform the following tasks to customize color mapping:

1. From the 5250 Settings tab, select **Advanced** against Custom Colors and select the check box against **Option Menu**, as shown in Figure 4-35.

The screenshot shows the 'Global IBM Terminal Settings' dialog box with the '5250 Settings' tab selected. The 'Custom Colors' dropdown is set to 'Advanced'. In the 'Allow use of' section, the 'Option Menu' checkbox is checked. Other settings include 'Key Mapping' set to 'Enabled', 'Keypad Capability' set to 'Yes', 'Record/Playback' set to 'Hidden', 'Command menu' set to 'Hidden', 'Print menu' set to 'Hidden', 'Font menu' set to 'No, no resize/move', '132 Columns' checked, 'Column Separators' unchecked, 'Desktop file' set to 'Yes', and 'Edit Menu', 'Control Menu', 'Help Menu', and 'Misc Prefs' all unchecked. The 'Emulator User ID', 'Emulator Password', and 'Other Parameters' fields are empty. The 'OK' and 'Cancel' buttons are at the bottom right.

Setting	Value
Key Mapping:	Enabled
Keypad Capability:	Yes
Record/Playback:	Hidden
Custom Colors:	Advanced
Appearance	
<input checked="" type="checkbox"/> 132 Columns	
<input type="checkbox"/> Column Separators	
Desktop file:	Yes
Emulator User ID:	
Emulator Password:	
Other Parameters:	
Allow use of	
Command menu:	Hidden
Print menu:	Hidden
Font menu:	No, no resize/move
<input type="checkbox"/> Edit Menu	
<input checked="" type="checkbox"/> Option Menu	
<input type="checkbox"/> Control Menu	
<input type="checkbox"/> Misc Prefs	
<input type="checkbox"/> Help Menu	
<input type="checkbox"/> New Session IP Window	

Figure 4-35 Neoware Connection Manager: 5250 Settings tab



2. Restart the 5250 console session for the changes to take effect. After the restart, the Option menu (Figure 4-36) is available in the 5250 session.

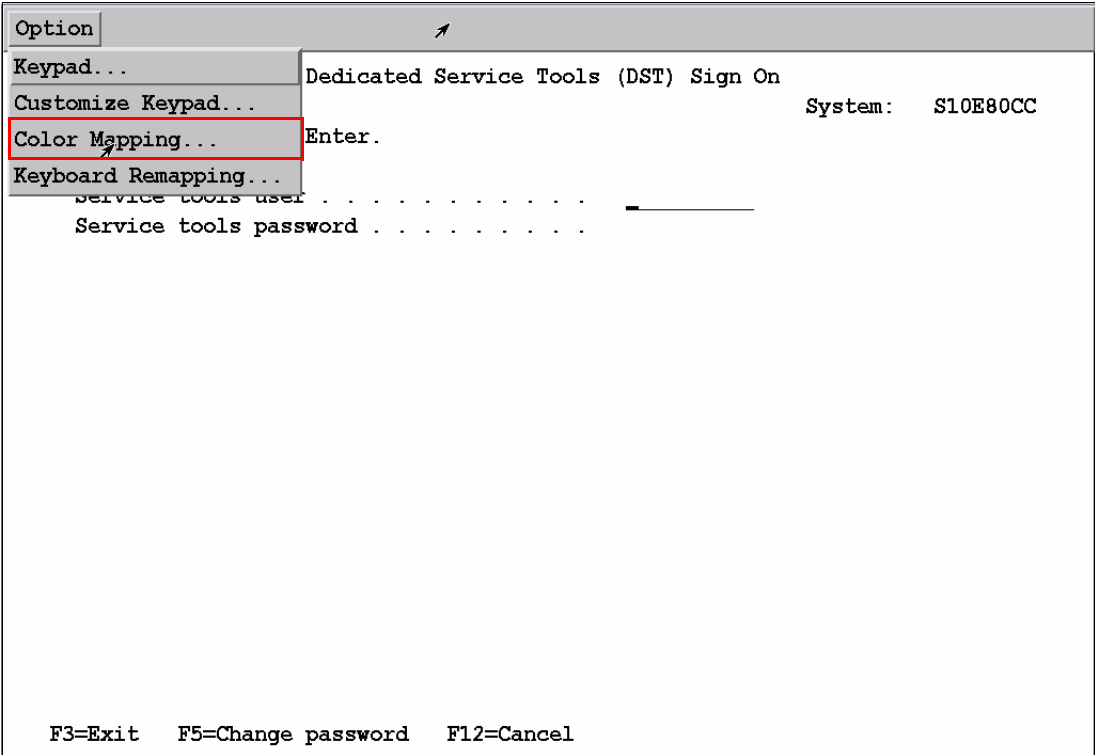


Figure 4-36 5250 Session color mapping

3. Click **Advanced**. Select a construct from the left column and change it to the color of your preference. Click **Apply Current Color**. When you are finished, click **Save** to save your changes to a new, user-defined color scheme (Figure 4-37).

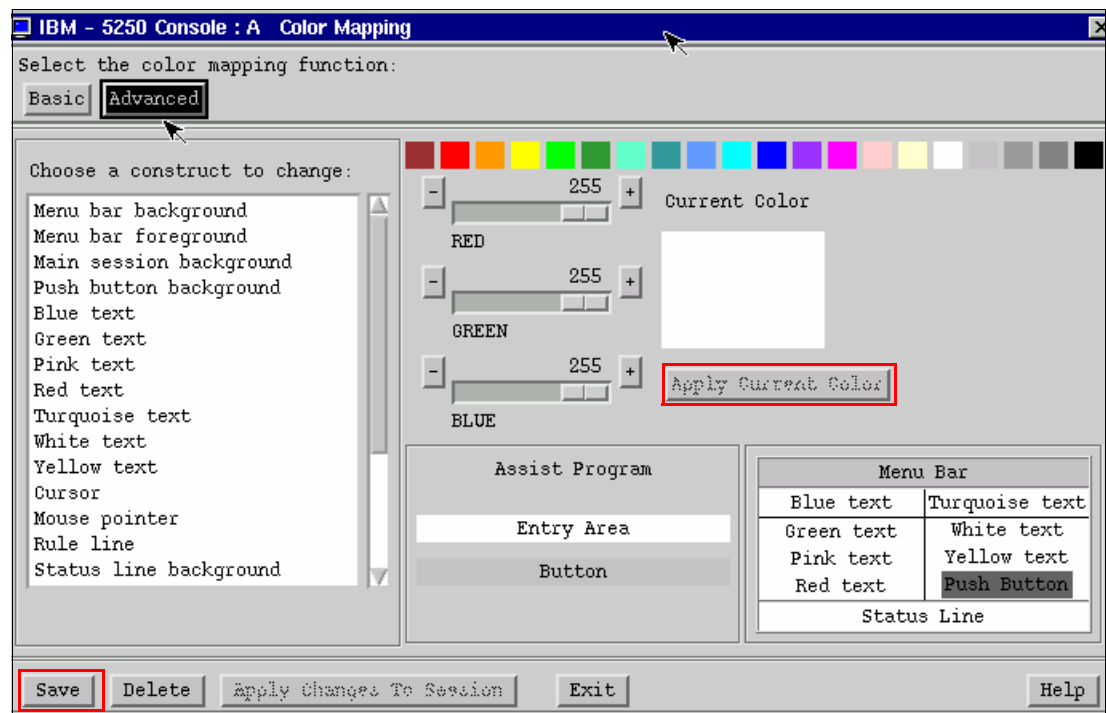


Figure 4-37 5250 session color mapping function

- Click **Basic**, select the new color scheme you just created and click **Save**, as shown in Figure 4-38.

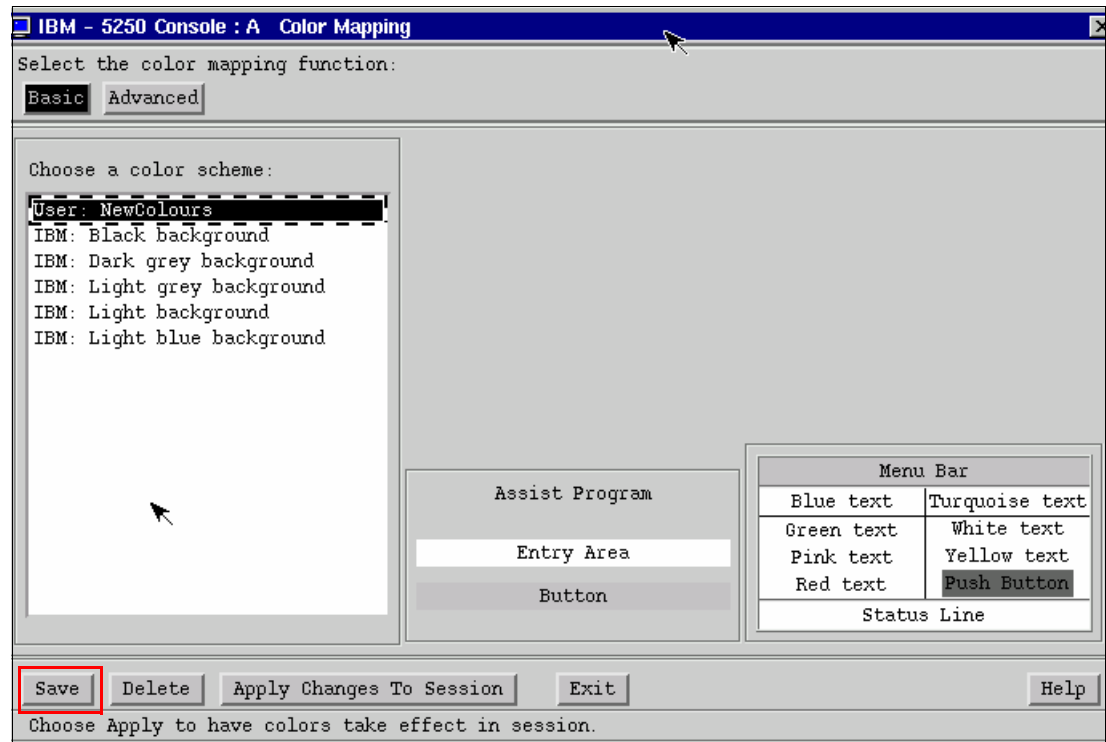


Figure 4-38 5250 session: Save color scheme

- Save the color scheme as the default for all your sessions, as shown in Figure 4-39.

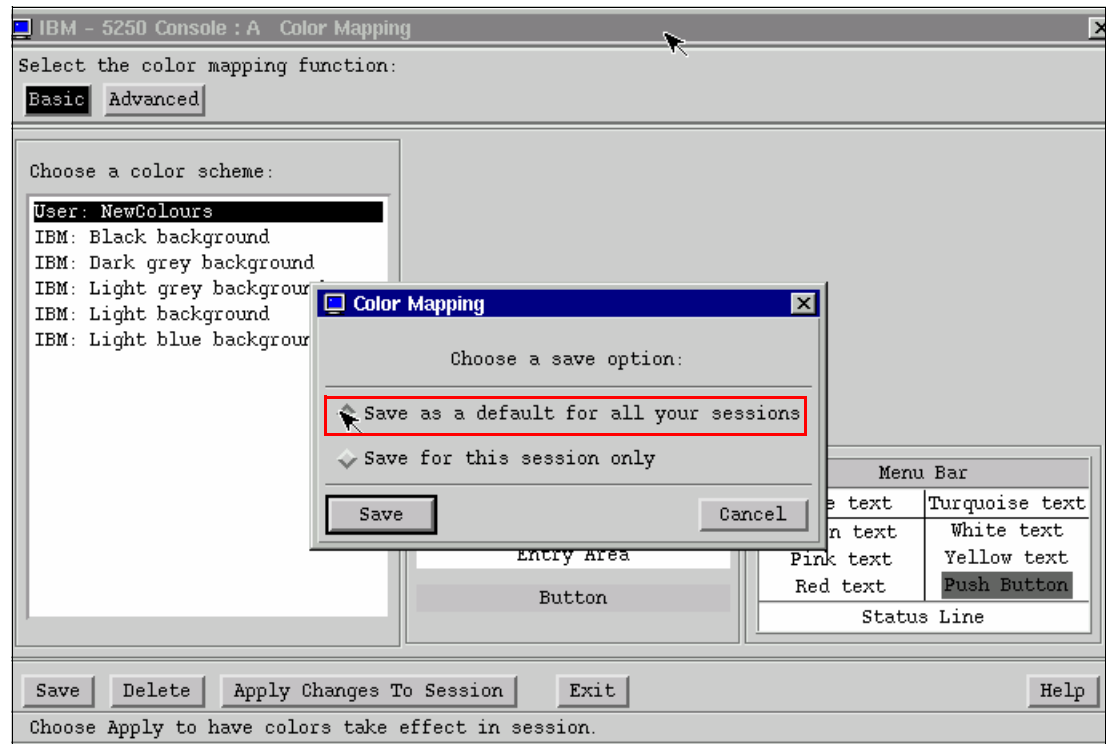


Figure 4-39 5250 session: Save option

6. When you exit the window, you will be asked whether to apply the changes you just made to the current session. Select **Apply changes to this session before exiting** and click **Exit** (Figure 4-40).

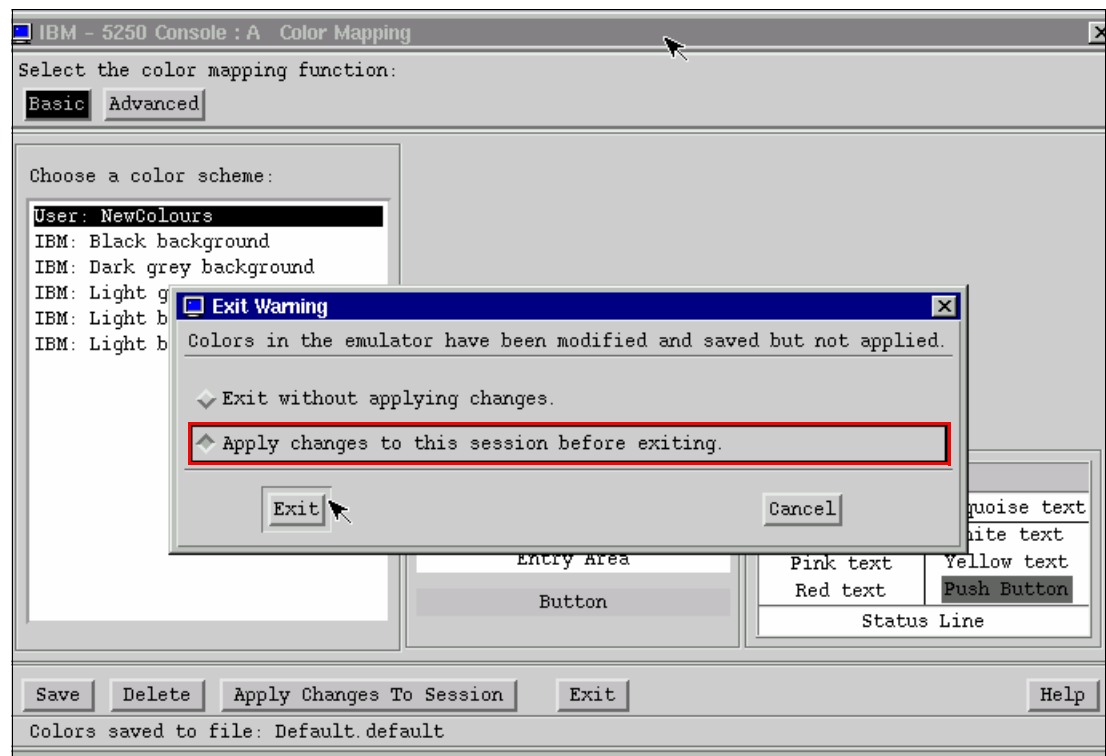


Figure 4-40 5250 session: Apply changes

7. At this point, you still have the Option menu in the top left corner of the 5250 session. Switch back to the Neoware Connection Manager to take the Option menu out of the 5250 session (Figure 4-41).

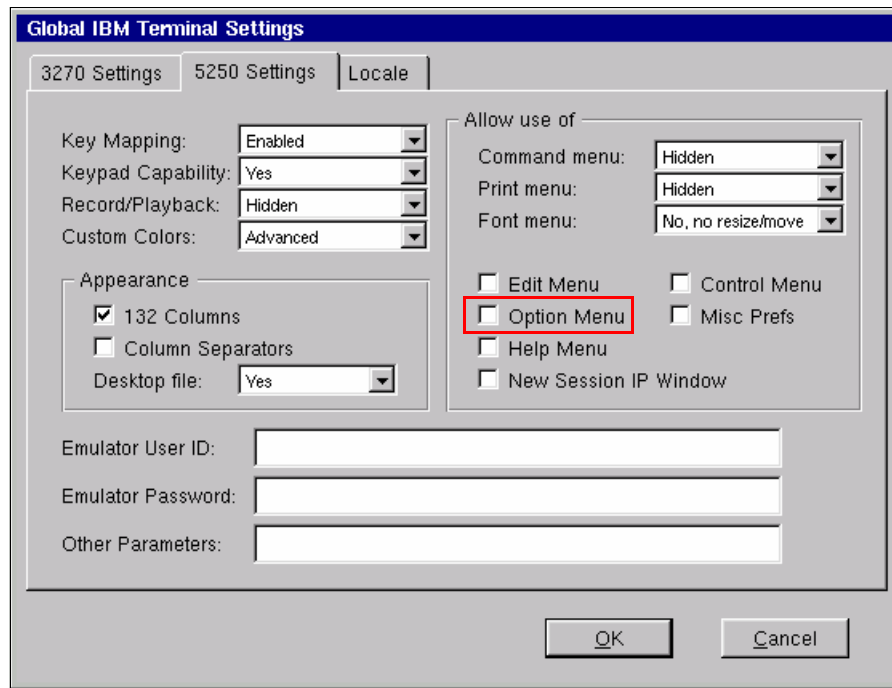


Figure 4-41 5250 settings

## 4.2.7 Maintenance

Hardware warranty replacements are made by Neoware. Customers must register at the following Neoware Web site for warranty entitlement:

<http://www.neoware.com/support/warranty.php>

The software service is delivered by Neoware. Currently, no known fixes are required for the Thin Console. Neoware provides fixes to its registered customers. Load that code to a USB memory key. The minimum capacity requirement for the memory key is 100 MB. The flash code contains the complete NeoLinux image, and not just a fix or update. Refer to the following Web site for more details:

<http://www.neoware.com/>

Perform these tasks to update (flash the code of) the Thin Console:

1. Receive the code from Neoware.
2. Expand the compressed file contents into the root directory of your USB key. If your USB key is shown as "E:" drive, E:\image.dd must be on the drive after the copy is complete. If you have already made a bootable USB key for Thin Console updates, you only require a new image.dd file. The file you receive might have a different format, such as image-142.dd. In such a situation, change the name to image.dd.
3. Find the batch file that corresponds to your mounted USB key drive letter. In this example, the USB key is located in E:. Double-click the corresponding batch file:
  - If your drive is mounted on E:, double-click **E:\syslinux32\sylslinux-e-drive.bat**.
  - If your drive is mounted on F:, double click **F:\syslinux32\sylslinux-f-drive.bat**.

- If you have another drive letter, either create a corresponding bat file using Notepad or contact Development.
- 4. Your USB key must now be a bootable installer.
- 5. Power down the Thin Console by holding down the Power button for five seconds.
- 6. Insert the USB key into your Neoware Thin Console.
- 7. Power on the Thin Console and press the Delete key after you hear the Thin Console beep to enter the BIOS setup utility.
- 8. In the Phoenix - AwardBIOS CMOS Setup Utility screen (Figure 4-42), select **Advanced BIOS Features**.



Figure 4-42 Phoenix - AwardBIOS CMOS Setup Utility

9. This takes you to the Advanced BIOS Features window (Figure 4-43).

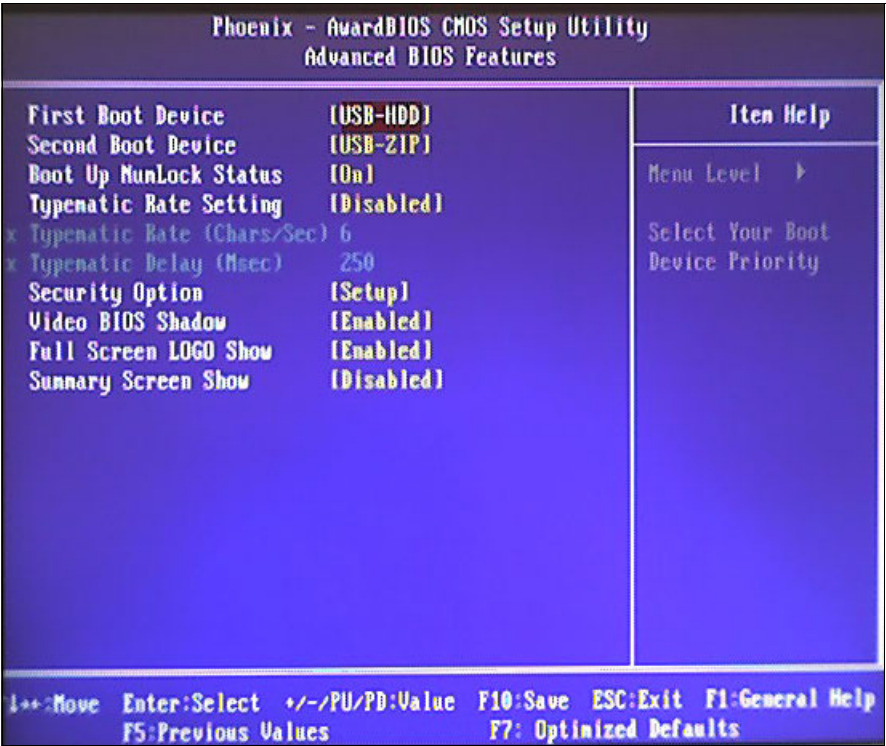
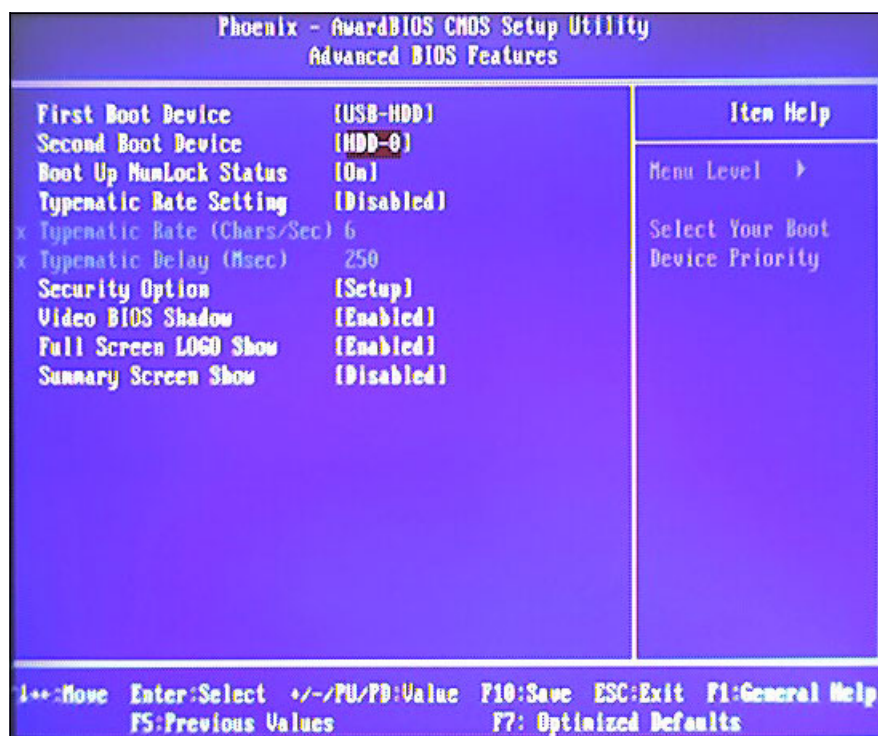


Figure 4-43 Advanced BIOS Features screen

- The First Boot Device is set to USB-HDD
- The Second Boot Device is set to HDD-0

Press F10 to save your BIOS changes, and press Enter to confirm **SAVE to CMOS and EXIT**.



*Figure 4-44 Boot devices*

11. The Neoware Thin Console recognizes the memory key and boots from it. You will receive the following message:

The image on the console is about to be overwritten.  
Do you wish to proceed with the update? [yes/no]

12. Reply yes to the message and press Enter. Follow the instructions when the following message is displayed on the screen:

Please remove the USB key and press Enter...



13. In the next screen (Figure 4-45), select a keyboard language.

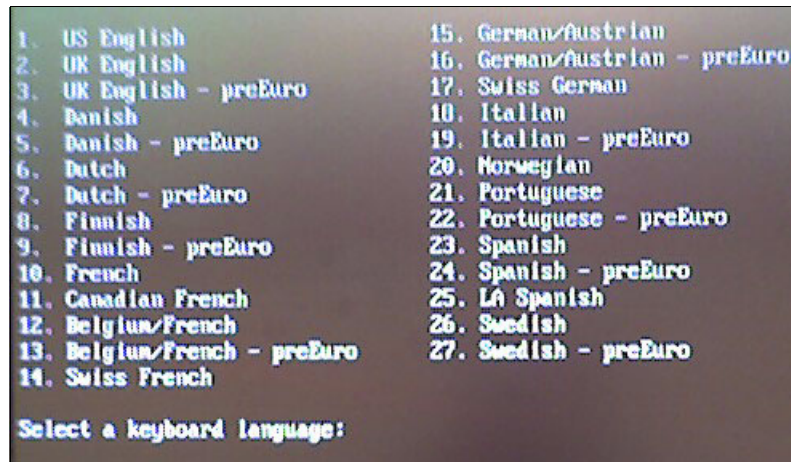


Figure 4-45 Keyboard language

14. When the connection status screen is displayed, the update is complete.

## 4.2.8 Backup/recovery and availability considerations

No backup tools are provided with the Thin Console. The Linux image is a stable environment, but if you ever find yourself in a situation where you have to recover a corrupted image, the procedure is to flash the Thin Console with the image that is available for download from the Web. Refer to 4.2.7, “Maintenance” on page 119 for more details.

Reloading the image implies a reset to factory settings, meaning that your customizations are lost. However, because the user-definable settings in the Thin Console are minimal, they can be easily re-entered in the event of a Linux image reload.

As with any other 5250 console type, an unplanned outage of the Thin Console hardware must not prevent the attached server from continuing to run. However, it will restrict access to some functionality on the system, such as the DST.

## 4.2.9 Troubleshooting

This section discusses solutions for some common problems.

### Hardware problems

Table 4-3 lists some common hardware problems that might occur when using the Thin Console. You can also refer to the documentation that comes with your console device or refer to the following Web site:

<http://www.neoware.com/>

*Table 4-3 Troubleshooting: hardware problems*

Symptom	Problem and recovery task
The display of the Thin Console is completely blank.	There might be a hardware problem with the Thin Console or monitor, or there might be a setup problem. Follow these steps to resolve the problem: <ol style="list-style-type: none"><li>1. Verify that the cabling is secure and accurate.</li><li>2. Verify that the Thin Console and monitor are powered on.</li><li>3. Reset the default monitor resolution setting. Refer to the console documentation or visit <a href="http://www.neoware.com/">http://www.neoware.com/</a></li></ol>
The keyboard is not working correctly.	This might be a hardware problem or it might be that the keyboard is set to a location that does not match the current keyboard setting. Refer to the console documentation or visit <a href="http://www.neoware.com/">http://www.neoware.com/</a>
You cannot view wide displays such as spool files using the 5250 console.	Set the resolution of the Thin Console to 1024 x 768.

## Connection status codes

Table 4-4 shows connection status code problems that might arise when using the Thin Console.

Table 4-4 Troubleshooting: using status codes

Symptom	Problem and recovery task
The status screen does not get past status code 00.xx	<p>The Thin Console is not able to find an active service processor. To resolve the problem:</p> <ol style="list-style-type: none"> <li>1. Verify that the Ethernet cable is plugged into either the HMC1 or HMC2 port at the back of the server.</li> <li>2. Verify that the Ethernet ports on both the server and the Thin Console are showing link-active and activity lights.</li> <li>3. Verify that the HMC port on the server is configured with either the 192.168.3.147 or the 192.168.2.147 IP address (manufacturing defaults). If the port is not configured using one these IP addresses, reset the factory settings. From the ezConnect - Neoware Connection Manager window, select <b>Settings</b> → <b>Appliance properties</b> → <b>Factory Reset</b>.</li> <li>4. Verify that the service processor is powered on by noting whether the control panel display is active.</li> <li>5. Restart the Thin Console to see whether the problem is reproducible.</li> <li>6. Isolate faulty hardware problems by using the other HMC port at the back of the server, using another Ethernet cable, or by using another Thin Console.</li> </ol>
The status screen displays status code 10.xx, and then prompts you for the HMC access password. After entering the password, the user ID and password cannot be authenticated.	<p>Complete these tasks to resolve the problem:</p> <ol style="list-style-type: none"> <li>1. Verify that the keyboard is set to a location that matches the current keyboard setting.</li> <li>2. Verify that the Caps Lock, Num Lock, and Scroll Lock keys are off.</li> <li>3. Change the HMC access password to a new value by logging into ASMI as the administrator. Refer to the topic on Changing ASMI passwords in the IBM Systems Hardware Information Center.</li> <li>4. Use a password with only uppercase English alphabetic characters. If this resolves the problem, contact IBM support.</li> </ol>
The status screen does not get past status code 10.xx or 20.xx.	<p>Complete these tasks to resolve the problem:</p> <ol style="list-style-type: none"> <li>1. Verify that another Thin Console or an HMC is not connected alongside this Thin Console.</li> <li>2. Restart the Thin Console to see if the problem is reproducible.</li> </ol>
The status screen does not get past status code 30.xx.	<p>The Thin Console displays status code 30.xx until the server is powered on and PHYP standby is reached. If the Thin Console remains in state 30.xx, power on the server. If the state is 0x0F and the status does not display system status after you see 30.xx, contact IBM support.</p>
The status screen does not get past status code 40.xx.	<p>Verify that another Thin Console or an HMC is not connected alongside this Thin Console. If so, disconnect the other console device.</p>

Symptom	Problem and recovery task
The status screen does not get past status code 50.xx.	Remaining in this state means that the Thin Console has completed the initialization of the firmware communication and has not successfully started communication with the LIC in i5/OS.

You can find this information in the IBM Systems Hardware Information Center at:

<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/iphc1/iphc1troubleshooting.htm>

## 4.3 Console card locations

Starting from V5R3, only the currently configured console type is supported. So if you are planning a migration or upgrade that includes a console-type change, predefine the new console type. Refer to 2.2.5, “Model 840 to model 570 (system upgrade with no LPAR or Hardware Management Console)” on page 45 for instructions.

In a partitioned environment, if no console type is specified, it scans the tagged IOP specified during the creation of the partition. If more than one console type is connected to this IOP, the first console device to connect becomes the console, thus making it difficult to predict which card will be chosen for each IPL.

Tagging the same IOP for both the primary console and the alternate console might result in the inability to select a console.

On systems where more than one console card location is available, you should not have two of the same card types occupy those locations per console mode. For example, if the console mode was set to 3 (for LAN), ensure that a LAN card is *not* installed in both the primary location and the alternate location.

### 4.3.1 Designated slots for models 5xx (V5R3)

Table 4-5 lists the designated slots for models 5xx (not 520+), in the order of priority.

Table 4-5 Designated slots for models 5xx (V5R3)

Model	Console slots for LAN and workstation IOAs (such as twinax) <sup>a</sup>	Async/ECS slot
520	C5 C2	C3
550	C4 If an IXS card takes this slot, LAN and twinax will not be available.	C2 If an IXS card is installed, it causes this location to go to C5 to make room for an IOP.
570	C4 C6 In the case of multiple CECs, these are in the same CEC as the load source.	C2
595	C04 (on #9194 Base PCI-X I/O enclosure)	C02 (#9194 Base PCI-X I/O enclosure)

a. Twinax adapters are typically placed in one of the Operations Console LAN slots but can replace the async card too.

### 4.3.2 i5/OS V5R3M5 and V5R4 (new Smart IOA plus+ models)

#### LAN console: Embedded LAN ports

In the new smart IOA (IOP-less) models, feature codes #5706 (PCI-X Gbps Ethernet-TX IOA) and #5707 (PCI-X 1 Gbps Ethernet-SX IOA) are the only console-supported smart IOAs.

The embedded port is the manufacturing default for the LAN console. Card locations are supported only when the embedded port is disabled.

Table 4-6 shows the location of the embedded LAN ports on models 520+, 550+, and 570+.

Table 4-6 5xx+ embedded LAN port location code

System	Location code of embedded LAN port
520	U787A.001.sssssss-P1-T5
550	U787B.001.sssssss-P1-T9
570	U7879.001.sssssss-P1-T6 In case of multiple CECs, the CEC with the load source

#### Designated slots 520+

Table 4-7 lists the designated slots for models 520+.

Table 4-7 Designated slots for models 520+

	HMC or IOP-less LAN without an IXS	HMC or IOP-less LAN with an IXS	Direct cable/twinax or IOP-driven LAN without an IXS	Direct cable/twinax or IOP-driven LAN with an IXS
C1	IOP or IOP-less IOA	IOP or IOP-less IOA	IOP	IOP
C2	IOP-less IOA or IOP-driven IOA if C1 is IOP	ECS-PTF IOA LAN (if #5706/5707)	IOP-less IOA or IOP-driven IOA if C1 is IOP 2nd location for LAN or twinax	ECS, LAN, or twinax
C3	ECS-PTF	Feature IOP	Direct cable (IOP must be in C6) or IOP	Feature IOP
C4	IOP-less IOA	IOPless IOA	IOP-less IOA	IOPless IOA
C5	LAN (if #5706/5707)	IXS card	Twinax or LAN console (IOP must be in C3 or C6)	IXS card
C6	IOP-less IOA or feature IOP	IXS card overhang	IOP or IOP-less IOA	IXS card overhang

## 4.4 Changing the console type

Refer to the IBM Systems Hardware Information Center for instructions about how to switch between console types on a running system:

<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/topic/iphca/iphcabook.pdf>

### 4.4.1 Using the console service functions (65+21)

When you migrate to another system without predefining the console type, the system might not detect the new console type. The system reference code to signal this event is A600500x.

In this event, you can force the system to switch between the different console types until it finds the type that is connected. The way you to do this is to use the console service functions (65+21). These functions can be used on a HMC system or a non-HMC system.

It is recommended that you only use this function if you do not have another workstation available to recover from the error. A prerequisite to starting the procedure is to make sure that all hardware is configured correctly for the console type you want to connect (in the case of a partitioned system with HMC, make sure that you tagged the right IOP), and that the console device is working properly and is connected as required.

Another prerequisite is that the server has advanced far enough through the IPL for the console service functions to be available. If your system is not in manual mode, and the extended functions are not activated, or both, perform these steps:

1. Place the server in manual mode.
2. Select console function 25 and press Enter.
3. Select console function 26 and press Enter.

The console service functions (65+21) must be performed from the control panel or through the control panel function on the HMC or the Operations Console control panel GUI:

1. From the control panel (or the control panel function on the HMC or the Operations Console), enter the function 65.
2. Within 45 seconds, enter function 21. Otherwise, the system will not tie both the functions together and consider the function 21 as a regular force DST to console. If function 65 and function 21 are entered in less than 45 seconds, you must see SRC A6nn500A, where *nn* represents the current console type (you might have to enter function 11 to display the SRC):
  - 00: No console defined
  - 01: Twinax console
  - 02: Direct-attached Operations Console
  - 03: LAN Operations Console
3. Enter function 65, followed by function 21 again to enter the edit mode. The operator panel displays SRC of A6nn500B to confirm the edit mode. You might have to enter function 11 to display the SRC. To cancel any changes and exit the edit mode, use function 66.
4. Repeat the functions 65+21(+11) until you reach the console type you require. (If you exceed 45 seconds between 65 and 21 when in the edit mode, SRC A6nn500D is presented, indicating a timeout condition. The system is no longer in edit mode.)
5. When you have reached the correct console type, enter only function 21(+11) to confirm your choice. SRC A6nn500C is displayed to indicate that the change is accepted.
6. Enter function 21 once more to force DST to the console.

An example of a console change would be changing from twinax (console type 01) to LAN console (type 03):

- ▶ 65+21+11 → A601500A → You are in display mode and the console mode is 01.
- ▶ 65+21+11 → A602500B → You entered edit mode and incremented the counter.
- ▶ 65+21+11 → A603500B → You incremented the counter again.
- ▶ 21+11 → A603500C → You invoked the action (set the console mode to 03).



## **i5/OS V5R4 software**

This chapter describes how to identify IBM software-licensed programs that may impact an iSeries migration to a new IBM System i5 and System i5+ hardware. It also identifies the supported upgrade paths and interoperability with existing systems.

## 5.1 i5/OS V5R4 software requirements and information

This section deals with some of the i5/OS V5R4-specific considerations for upgrades to the new model 5xx hardware:

- ▶ i5/OS V5R4 requires a minimum of 128 MB of main storage in each partition, with 256 MB in the primary partition. Additional main storage higher than these values might be required for acceptable system performance.
- ▶ i5/OS V5R4 requires that the load source disk in each OS/400 partition is 17 GB or larger.
- ▶ i5/OS V5R4 Licensed Internal Code (LIC) requires more storage space than the earlier releases. All of the partitions with V5R3M0 or earlier installed require additional storage space that is reserved before the installation.

**Important:** Failure to reserve additional space results in the upgrade stopping during the installation of the LIC.

- ▶ Before upgrading to i5/OS V5R4, some program temporary fixes (PTFs) must be installed in the current release. This enables additional options in the Prepare for Upgrade menu.

**Important:** These PTFs are shipped with the OS/400 release. If these PTFs are not installed and the software agreements are not accepted, the installation fails.

- ▶ Server firmware must be at release SF235\_160 or later.
- ▶ Check whether the Hardware Management Console (HMC) code level is compatible with the server firmware.

### 5.1.1 i5/OS V5R4 informational authorized program analysis report and PSPs

For additional information about new 5xx hardware and the required software, refer to the PSPs and the informational authorized program analysis reports (APARs):

<http://publib.boulder.ibm.com/infocenter/iseriess/v5r4/topic/rzaq9/rzaq9.pdf>

For additional information about the new functions and the functions that have been removed in i5/OS V5R4, refer to *iSeries Memorandum to Users Release R540*, which is available on the Web at:

[http://www-912.ibm.com/s\\_dir/sline003.nsf/2d3aff1c6b4d6ce086256453000d971e/bdb2077acff30ff28625710f005ca12f](http://www-912.ibm.com/s_dir/sline003.nsf/2d3aff1c6b4d6ce086256453000d971e/bdb2077acff30ff28625710f005ca12f)

APAR and PSP information can be found by using the following identifiers:

- ▶ SF98010 refers to installation information for i5/OS V5R4.
- ▶ SF99540 refers to information about problems discovered since the latest PTF cumulative package.
- ▶ MF99540 refers to information about installing V5R3 hardware.
- ▶ SF99168 refers to information about server upgrades and data migrations.



## 5.1.2 Required software

i5/OS V5R4 or V5R3M5 is a prerequisite on all partitions for the new System i5+ hardware. Install the latest cumulative PTF package, HIPER PTFs, and any hardware-specific PTFs for your installation on all of the partitions.

Enter the command `SNDPTFORD PTFID(SF99540) DLVY(*ANY)` to order the latest cumulative PTF package. This package must have the latest group HIPER PTFs and database PTFs delivered with it.

## 5.1.3 AS/400 models not supported in i5/OS V5R4

Older AS/400 models are not supported in i5/OS V5R4:

- ▶ AS/400 models 4xx and 5xx are only supported up to OS/400 V5R1.
- ▶ AS/400 models 150, 6xx, Sxx, and SB1 are only supported up to OS/400 V5R2.
- ▶ iSeries models 170 and 7xx are only supported up to i5/OS V5R3.

**Tip:** Clients with these models must perform data migration to new 5xx models rather than following the upgrade path.

It is preferable for clients to upgrade to the latest supported level on the hardware for interoperability. If this is not possible (due to hardware, insufficient memory, or time constraints, for example), data migration can be performed from the current release.

i5/OS V5R4 is the last release that will support models 270, 820, 830, 840 SB2, and SB3.

## 5.1.4 License agreements

In i5/OS V5R3, V5R3M5, and V5R4, software license agreements must be accepted before certain products can be installed. It is essential that you agree to the LIC and OS/400 software agreements; otherwise, the installation fails.

### Agreeing to licenses before installing the licensed programs

Perform the following tasks:

1. Ensure that the software agreement PTFs have been applied.
2. Ensure that a custom installation list is created.
3. Run the `GO LICPGM` command.
4. Select option **5** (Prepare for install).
5. Select the **Work with Software agreements** option.
6. Select all of the agreements that you want to accept and press Enter.
7. Press F14 to accept each agreement.

## 5.2 i5/OS V5R4 software upgrade paths

Some releases of OS/400 may not be upgraded directly to i5/OS V5R4:

- ▶ Direct upgrade to i5/OS V5R4 can be performed only from releases OS/400 V5R2, i5/OS V5R3M0, and V5R3M5.
- ▶ Systems at releases prior to OS/400 V5R2 must perform a two-step upgrade, first upgrading to release OS/400 V5R2 or i5/OS V5R3, and then upgrading to i5/OS V5R4.

**Important:** All V5 releases (V5R1, V5R2, and V5R3) require a *minimum* of 128 MB of main storage in each partition (V5R3 requires a *minimum* of 256 MB in the primary partition). Additional storage above these minimums might be required for reasonable system performance.

When upgrading across more than one release, refer to iSeries Memorandum to Users Release R540 and the PSP information for each of the skipped releases to see how your installation might be affected.

## 5.3 Interoperability with the existing systems

The movement of data between systems or partitions at different operating system levels is sometimes required. The support for this is called interoperability, which also allows for applications to be compiled at either release and allows transparent communication between systems. It supports centralized management facilities and allows support for PCs running at various levels of client access. i5/OS V5R4 has interoperability with OS/400 V5R2 and later.

## 5.4 i5/OS V5R4 software upgrade

This section outlines the i5/OS V5R4 software upgrade process. Ensure that care is taken because there are differences from the previous release upgrades.

**Important:** This section is only an outline. It is assumed that automatic installation from CD is performed. For details about the installation process or alternative methods, refer to *i5/OS and Related Software - Install, Upgrade, or Delete. Version 5 Release 4*, SC41-5120, at <http://publib.boulder.ibm.com/infocenter/iseriess/v5r4/topic/rzahc/rzahc.pdf>

### Pre-upgrade planning

The following tasks are involved in pre-upgrade planning:

1. Check whether your server meets the requirements to support the new release.
2. Confirm the delivery of all the required software components and license keys.
3. Order the most recent Cumulative PTF package and Group PTF package that are relevant to your environment.
4. View the PSP for the current release and the target release.
5. Identify required software fixes (software acceptance PTFs and others identified by the PSP).
6. If you have nonconfigured disks, a PTF that enables you to set the disk configuration option exists.
7. Print a list of all the system values.
8. Gather performance data.
9. Ensure that the server has sufficient disk storage space.
10. Ensure that the load source disk is 17 GB or larger on each partition.
11. Ensure that IBM-supplied product libraries are not in a user ASP.
12. Ensure that there are no user-created subdirectories in the /QIBM/ProdData/CA400/Express path or the /QIBM/ProdData/ path.

13.Delete the PTF cover letters in QGPL/QAPZCOVER.

### Preparing the server in the current release

The following tasks are involved in preparing the server in the current release:

1. Load and install the PTFs identified earlier.
2. Permanently apply all of the PTFs.
3. Change the system values QSYSLIBL and QUSRLIBL to remove any licensed program libraries or secondary language libraries. Do not remove libraries QSYS, QGPL, QUSRSYS, QTEMP, or QSYS2.
4. Change the system value QALWOBJRST to \*ALL.
5. Change the system value QVFYOBJRST to 3.
6. Set the time zone data area.
7. Verify the system objects.
8. Ensure two-phase commit integrity.
9. If there are a lot of spool files on the system, set the compress job tables IPL attribute to none. To view, enter:

```
DSPIPLA CPRJOBATR
```

To change, enter:

```
CHGIPLA CPRJOBATR(*NONE)
```

- 10.Enter the following command and select option 5:

```
GO LICPGM
```

- 11.Create a customized list of software to install with the option.
- 12.Check for items not found on the media.
- 13.Add any additional programs to the list.
- 14.Delete any unsupported products.
- 15.Delete any products or product options that are no longer required.
- 16.Accept the software agreements.
- 17.Clean up the disk storage space and remove unwanted products and data.
- 18.Allocate additional space for LIC.

**Important:** The additional space is reserved during the next IPL. This IPL must occur prior to upgrading (a required step for each partition).

- 19.If you have nonconfigured disks, set the Keep disk configuration option to \*YES.
- 20.Set the console mode in the DST.
- 21.If you are upgrading IBM Cryptographic Access Provider 128-bit, and currently have 40-bit or 56-bit versions installed, remove them.
- 22.Vary off Integrated xSeries servers and other application servers such as Lotus Domino servers.
- 23.Check whether the installation device you want to use is available to this partition and is a suitable alternative IPL device.

## Performing a full system save

To perform a full system save, type the following command:

```
GO SAVE
```

Select option **21**.

**Important:** After you begin to upgrade the Licensed Internal Code (LIC) to the next release, the process must complete. If it is not possible to complete the upgrade, you will have to recover your system by scratch installing from this backup.

During the installation process and subsequent PTF installation, the system may have to IPL several times. You can prevent the system from running your autostart jobs by changing the system value QSTRUPPGM to \*NONE.

## Performing an automatic upgrade

The steps involved in performing an automatic upgrade are:

1. Insert the System LIC CD into the CD drive.
2. Set the control panel mode to Normal.
3. Power down the server or partition by entering the following command:  

```
PWRDWN SYS OPTION(*IMMED) RESTART(*YES) IPLSRC(D)
```
4. Load the next volumes when prompted.

## Verifying the success of an automatic installation

Perform the following tasks to verify the success of an automatic installation:

1. When the sign in display is shown, sign in as QSECOFR.
2. Enter the command GO LICPGM, select option **50**, and press Enter.
3. In the Display Install History screen, press Enter.
4. Check the displayed log for errors.
5. Refer to Chapter 10, "Troubleshooting software installation problems" in *System i i5/OS and related software: Installing, upgrading, or deleting i5/OS and related software, Version 5 Release 4*, SC41-5120, which is available on the Web at:  
<http://publib.boulder.ibm.com/infocenter/iseriess/v5r4/topic/rzahc/rzahc.pdf>

## Installing additional programs, if required

To install additional programs, perform the following tasks:

1. Enter the GO LICPGM command and select option **11** (Install licensed programs).
2. Select the required options.

**Tip:** If the required option or program is not in the list, go to the blank line at the top of the list and add the program identifier.

3. Insert CDs as required.

## Installing secondary languages, if required

To install the secondary languages, perform the following tasks:

1. Enter the command GO LICPGM and select option **21** (Install secondary languages).
2. Place the CD in the drive.

3. Select the language you require.

## **Installing PTFs**

To install PTFs, perform the following tasks:

1. Insert the first Cumulative Package CD.
2. Enter the command GO PTF and select option **8**.
3. Insert the other CDs when prompted.
4. IPL PWRDWN SYS OPTION(\*IMMED) RESTART(\*YES) IPLSRC(B)I.
5. Wait for the INZSYS to complete.
6. Install the HIPER, DATABSE, and PTF groups that are relevant to your installation.
7. IPL PWRDWN SYS OPTION(\*IMMED) RESTART(\*YES) IPLSRC(B).
8. Verify the correct installation of the PTFs by running the GO LICPGM command and selecting option **50**.

## **Preparing the system for normal use**

Follow these steps to prepare the system for normal use:

1. Change the system values back to their original settings (with the help of the printout you took earlier); in particular, reset QSYSLIBL, QUSRLIBL, QVFYOBJRST, QALWOBJRST, and QSTRUPPGM.
2. Set CHGIPLA CPRJOBATR back to its previous value.
3. Perform a test.
4. Return the system to the users.





## Tape data encryption in i5/OS V5R4

This chapter describes the new hardware-based tape encryption support available in i5/OS V5R4. The IBM TotalStorage TS1120 tape drive supports hardware-based encryption. The encryption key is supplied by an external key manager that can run either on i5/OS or on a Windows-based PC.

This chapter also describes the TS1120 and shows how to set up and use the Encryption Key Manager (EKM).

## 6.1 Using the Encryption Key Manager and TS1120 tape drive

Many clients are aware of possible ways to protect the system and the data on it to:

- ▶ Avoid data loss, which can be caused by a disaster such as fire or hurricane, or simply by a person accidentally deleting the wrong library.
- ▶ Protect the confidentiality of data from malicious intrusion or even theft.
- ▶ Comply with governmental security regulations such as the Sarbanes-Oxley Act (SOX).

The following means of physical security and logical security can help accomplish these needs:

- ▶ High Availability (HA) and disk mirroring solutions
- ▶ Journaling
- ▶ Daily backups
- ▶ Site security
- ▶ Network security (firewall)
- ▶ i5/OS built-in security functionalities

When you encrypt your data, you take this a step further. Not only does encryption protect your data from accidental loss, such as somebody erasing active data from a tape, but also from deliberate compromise, including a theft of tapes during transport to or from a tape vaulting facility, or unauthorized personnel accessing confidential data stored on tape. However, even as you build this level of security, you want to be able to share parts of the confidential data with trusted parties such as clients and partners.

Until now, tape encryption for the System i environment was possible only by implementing third-party solutions. The following Web site provides an overview:

<http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100790>

Another solution is now available, based on a new encryption-capable tape drive, the TS1120. The encryption is managed by the TS3500 tape library. The section that follows looks at tape encryption methods.

### 6.1.1 Encryption methods

There are four ways to manage data encryption:

- ▶ System-managed, where data is encrypted by the host OS before being written to tape.
- ▶ Application-managed, where encryption of data is performed by a specific application, possibly running on another system. An example of an IBM application that can manage encryption is IBM Tivoli® Storage Manager.
- ▶ Appliance-managed, where a hardware device sits between the host OS and the tape device. Data is encrypted as it passes through the appliance.
- ▶ Library-managed, where a tape library system manages the encryption of data, using the encryption capabilities of an attached tape drive.



## 6.1.2 Encryption components

The tape encryption solution presented in this section is library-managed. It is built on the following three components:

- ▶ The IBM Encryption Key Manager component for the Java platform. The EKM server is used to store and manage the keys that are used for encryption.
- ▶ The TS3500 tape library system (Figure 6-1) to manage the encryption. For i5/OS, the supported features are 3584-L22, L23, D22, and D23. For firmware updates, refer to:  
<http://www.ibm.com/servers/storage/support/lto/3584/downloading.html>



Figure 6-1 TS3500 tape library system

- ▶ The TS1120 encryption-capable tape drive (Figure 6-2) to perform the encryption. Only the model or type 3592-E05 can perform encryption. All the new orders are encryption capable. For existing models 3592-E05, a field upgrade for encryption can be ordered.

For more information, refer to:

<http://www-03.ibm.com/servers/storage/tape/ts1120/index.html>

Order 3592-E05 FC 9592 (plant) or FC 5592 (field). Order 3584 Lxx FC 9900 to use the library-managed encryption. For the IBM Customer Engineer (CE) setup of encryption drives, order 3592-E05 FC 9596 or FC 5596.



Figure 6-2 TS1120

### 6.1.3 Planning for tape encryption

Before you implement tape encryption with the IBM EKM, decide on which platform you will install the EKM server, and which type of keystore you will use. Refer to *IBM Encryption Key Manager component for the Java platform, EKM Introduction, Planning, and User's Guide*, GA76-0418. Also refer to 6.1.4, "Backup and recovery considerations with Encryption Key Manager" on page 140.

Regardless of which EKM server platform and keystore type you choose, each IBM EKM implementation with the TS1120 tape drive involves the following tasks. (Refer to 6.1.5, "Encryption Key Manager server on a PC" on page 142, 6.4, "Encryption Key Manager on i5/OS" on page 164, and 6.7, "Configuring your TS1120 tape drive for encryption" on page 184.)

1. Install the required operating system on your server.
2. Install the correct version of the Java Runtime Environment (JRE™) or IBM Software Development Kit (SDK) for Java.
3. Install the IBM Java unrestricted policy files (US\_export\_policy.jar and local\_policy.jar).
4. Install the IBM EKM Application (IBMKeyManagementServer.jar) and the IBM EKM Sample Configuration File (KeyManagerConfig.properties).
5. Install a tool to manage the type of keystore you have chosen.
6. Define the keystore and import or create keys into the keystore.
7. Configure EKM and define tape drives to EKM, or set the drive EKM configuration property .acceptUnknownDrives to on.
8. Start the EKM server.
9. Enable the TS1120 tape drive for encryption.

In this topic, only the installation of an EKM server on the System i platform and a Windows-based PC are discussed in detail. However, EKM is supported on a wide range of platforms. For installation on other platforms, refer to *IBM Encryption Key Manager component for the Java platform, EKM Introduction, Planning, and User's Guide*, GA76-0418.

You can find this and other publications, file downloads, and updated information on the IBM TotalStorage Web site under the TS1120 topic:

<http://www.ibm.com/servers/storage/support/tape/ts1120/downloading.html>

In the Support for TS1120 Drive page, click **Downloadable files**. In the page that is displayed, select **IBM Encryption Key Manager component for the Java Platform**.

### 6.1.4 Backup and recovery considerations with Encryption Key Manager

When planning for EKM, be sure to consider the backup and recovery implications.

Keys can get lost in two ways:

- ▶ The keystore itself is encrypted.
- ▶ The keys are corrupted or the system they are running on is down.

**Important:** The impact of losing your keys is nothing less than disastrous. *All data on the encrypted tapes become inaccessible, without any means of recovery. There are no "workarounds."*

In the light of the probable consequences, keep the following points in mind:

► *Do not encrypt the keys you require for decrypting.*

If you install your keystore on the same system from which you are backing up data, you risk backing up parts of the EKM to the encrypted tape as well. Although it might look easier to have your EKM server on the same system when all you want to do is restore just one library or a file, it will make your system *completely unrecoverable* if a scratch install is required. Therefore, it is recommended that you install the EKM server on a different system from the one on which you are encrypting data.

► *Do not encrypt data for which you do not require encryption.*

Consider what data you want to encrypt. LIC, i5/OS, system libraries, and directories do not contain confidential or sensitive data. Accidental loss can be covered by maintaining several copies of the system data. Do not encrypt data unnecessarily.

Combine these two recommendations, which can also help you save considerable time in the event of a complete system loss of your System i5. Because the EKM server is running on a different system, you can start recovering it independent of your System i5 server. At the same time, because you have not encrypted the system data on the System i5 server, you do not have to wait until the EKM server is up and running to start installing the System i environment in your recovery site. If your EKM server is going to be running the same system, you must first recover that system to a point where you can recover the EKM server if you have not encrypted any data up to that point.

► *Plan for redundancy.*

The critical part of your EKM server is the keystore that holds the keys. You can back it up to the media supported on the EKM server and keep this in a secured vault. However, because there is no recovery from lost keys, and because you cannot perform backup or restore functions if your only EKM server is down, it is recommended that you also build in redundancy by installing two EKM servers at least.

You can set up an EKM server on your Disaster Recovery (DR) site and synchronize it with the one on the main site. Alternately, you can just install a new EKM server on the DR site in the event of a real disaster or test disaster and import your keys into the keystore. Irrespective of the solution you choose, if you configure more than one EKM server, ensure that you run the same version of software and keystore type on both the servers, or alternately, test their compatibility.

As part of your Disaster Recovery Plan (DRP), make sure that you test the compatibility of the EKM servers and of the tape drives, because there is a possibility that the TS3500 tape library configuration at the DR site is different from yours. Configure the EKM server to recognize the new hardware, and configure the TS3500 tape library to point to the correct EKM server.

## 6.1.5 Encryption Key Manager server on a PC

This section describes the EKM program running on a PC desktop or a PC server.

### Software requirements

Table 6-1 shows the minimum Windows operating system versions and the minimum SDK version.

Table 6-1 Minimum software requirements for Windows

Operating system	Runtime environment bundled with IBM TotalStorage Productivity Center - Limited Edition (TPC-LE) - LPP 5608-VC6 <sup>a</sup>
Windows 2000, Windows 2003	<ul style="list-style-type: none"><li>▶ IBM 64-bit runtime environment for Windows on AMD64/EM64T architecture, Java 2, Technology Edition, V5.0</li><li>▶ IBM 32-bit runtime environment for Windows, Java 2, Technology Edition, V5.0</li><li>▶ IBM 64-bit SDK for Windows on Intel® Itanium® architecture, Java 2, Technology Edition, V1.4.2</li></ul>

a. This product can only be installed from CD. It is not available for download. For more information, visit <http://www.ibm.com/servers/storage/software/center/limited/index.html>

After you have the required Windows operating system and the correct IBM Java Runtime Environment (JRE) for Windows installed (refer to “Installing the IBM Java Runtime Environment for Windows” on page 143):

- ▶ Install the IBM Java unrestricted policy files (refer to “Installing the unrestricted policy files” on page 146).
- ▶ Install the IBM EKM Application and the IBM EKM Sample Configuration file (refer to “Installing the Encryption Key Manager .jar and sample configuration file” on page 147).
- ▶ Install the proper tool to manage the keys in your type of keystore. In this example, we define a JCEKS keystore. Valid tools to manage this are the iKeyMan utility or the standard Java tool, keytool (refer to “Installing the iKeyman utility” on page 148).

## Installing the IBM Java Runtime Environment for Windows

Perform the following tasks:

1. Load the correct CD from the IBM TotalStorage Productivity Center - Limited Edition (TCP-LE) - LPP 5608-VC6 and select the JRE you want to install. In this example, we install JRE V5.0 SR2 (Windows/IA32). When the installation wizard opens, click **Next**, as shown in Figure 6-3.

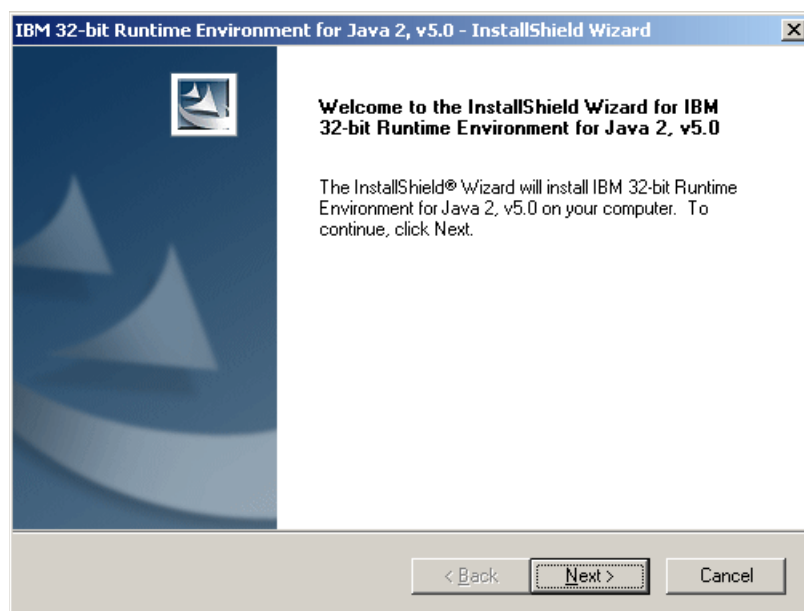


Figure 6-3 JRE InstallShield Wizard

2. Accept the license agreement.
3. The Choose Destination Location window (Figure 6-4) is displayed. You can change the destination folder if you want. Make a note of the folder path because you require it to start the EKM server at a later step. Click **Next**.

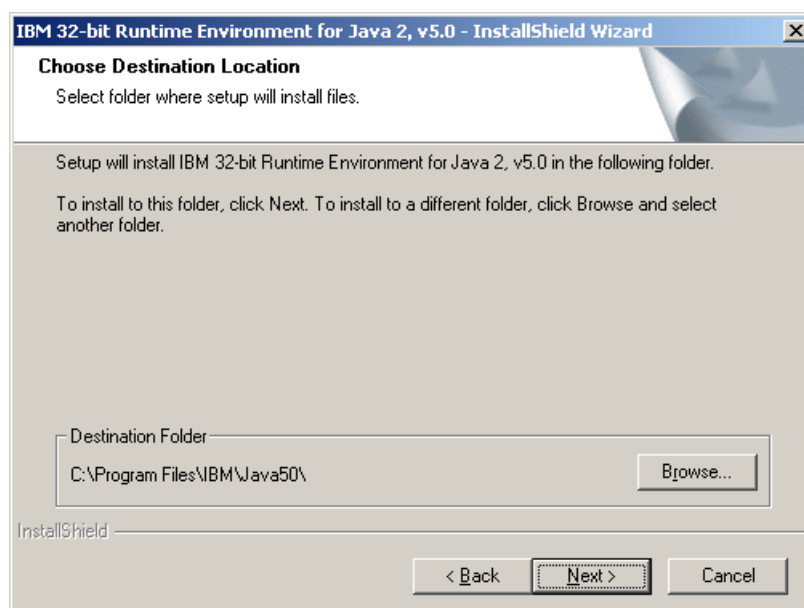


Figure 6-4 JRE destination folder

4. Click **No** when the installation wizard asks you whether you want to make this JRE the System JVM, as shown in Figure 6-5.

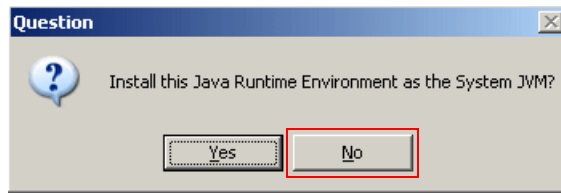


Figure 6-5 JRE as system JVM

5. The Start Copying Files window (Figure 6-6) is displayed. Click **Next**.

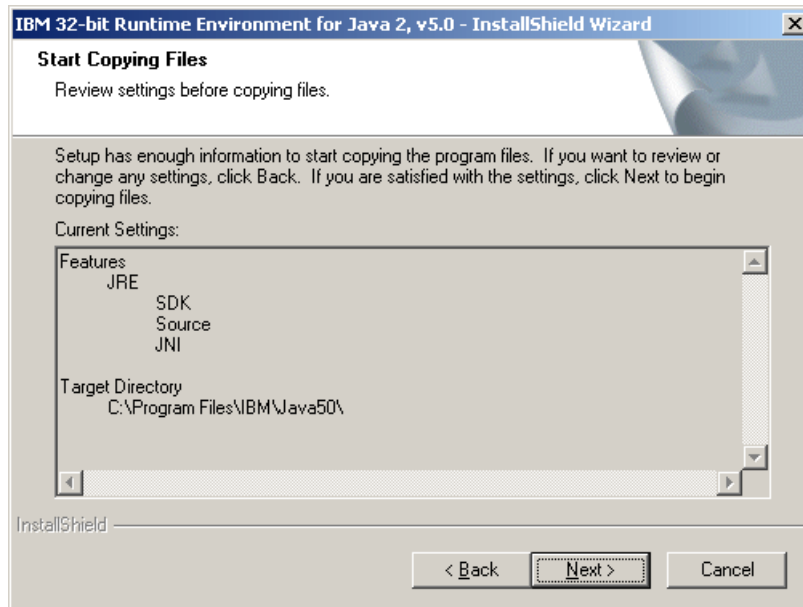


Figure 6-6 Start Copying Files window

6. The Browser Registration window (Figure 6-7) is displayed. Select a browser to be associated with EKM. Click **Next**.

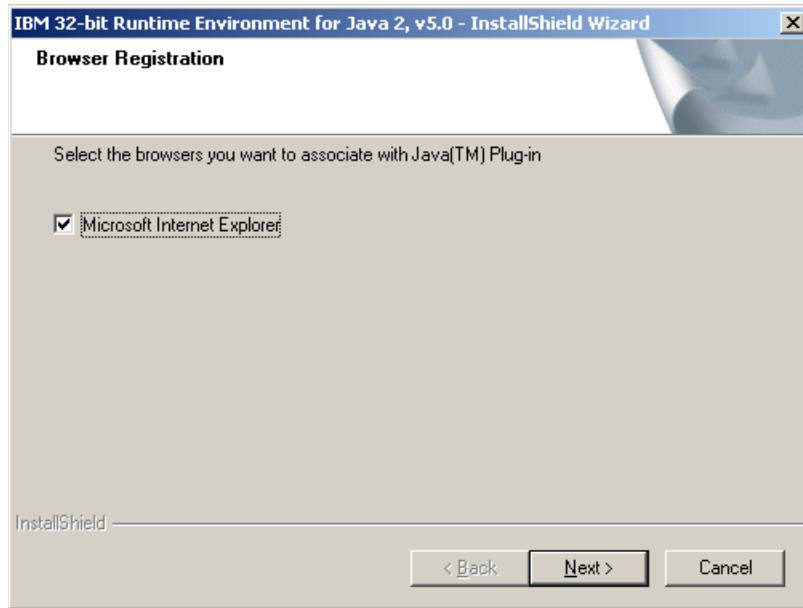


Figure 6-7 Browser Registration window

7. The InstallShield Wizard Complete window (Figure 6-8) is displayed. Click **Finish** to complete the installation.

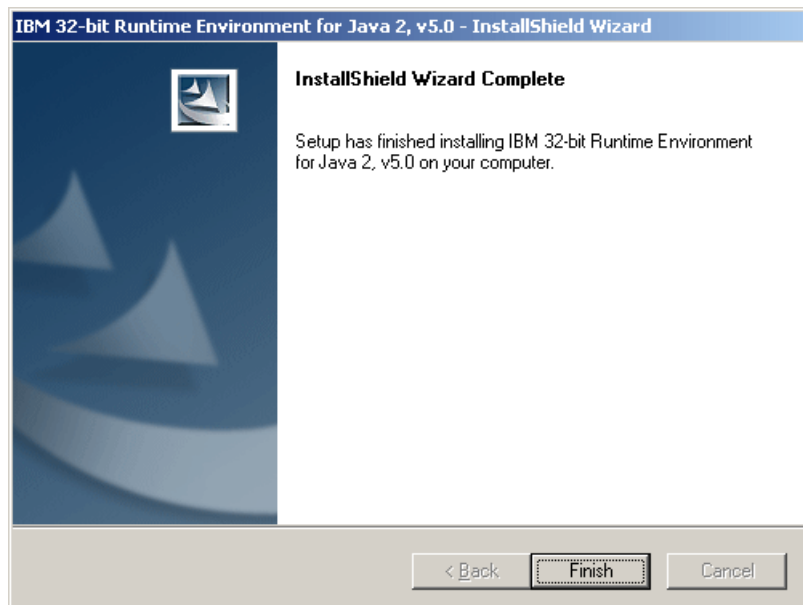
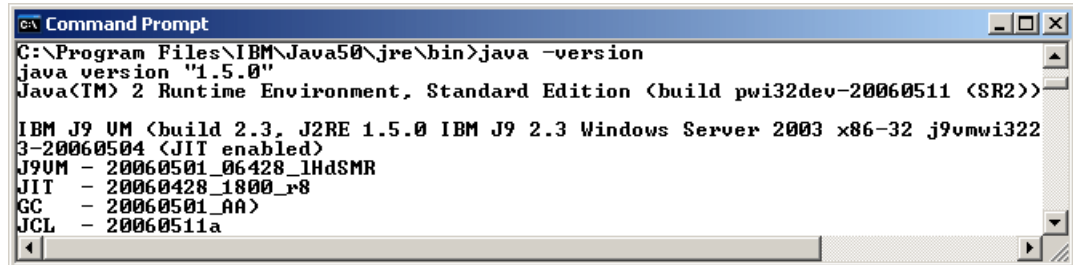


Figure 6-8 InstallShield Wizard Complete window

8. Verify the installation and version of the JRE by entering the following commands in a DOS prompt (Figure 6-9):

```
cd C:\Program Files\IBM\Java50\jre\bin
java -version
```



```
C:\Program Files\IBM\Java50\jre\bin>java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build pwi32dev-20060511 <SR2>)

IBM J9 UM (build 2.3, J2RE 1.5.0 IBM J9 2.3 Windows Server 2003 x86-32 j9vmwi322
3-20060504 <JIT enabled>
J9UM - 20060501_06428_1HdSMR
JIT - 20060428_1800_r8
GC - 20060501_AA>
JCL - 20060511a
```

Figure 6-9 Check version command prompt

## Installing the unrestricted policy files

Perform the following tasks:

1. Go to the following Web site, scroll down to the Java Cryptography Extension (JCE) topic (Figure 6-10) and click **IBM SDK Policy files**:

<http://www.ibm.com/developerworks/java/jdk/security/50>

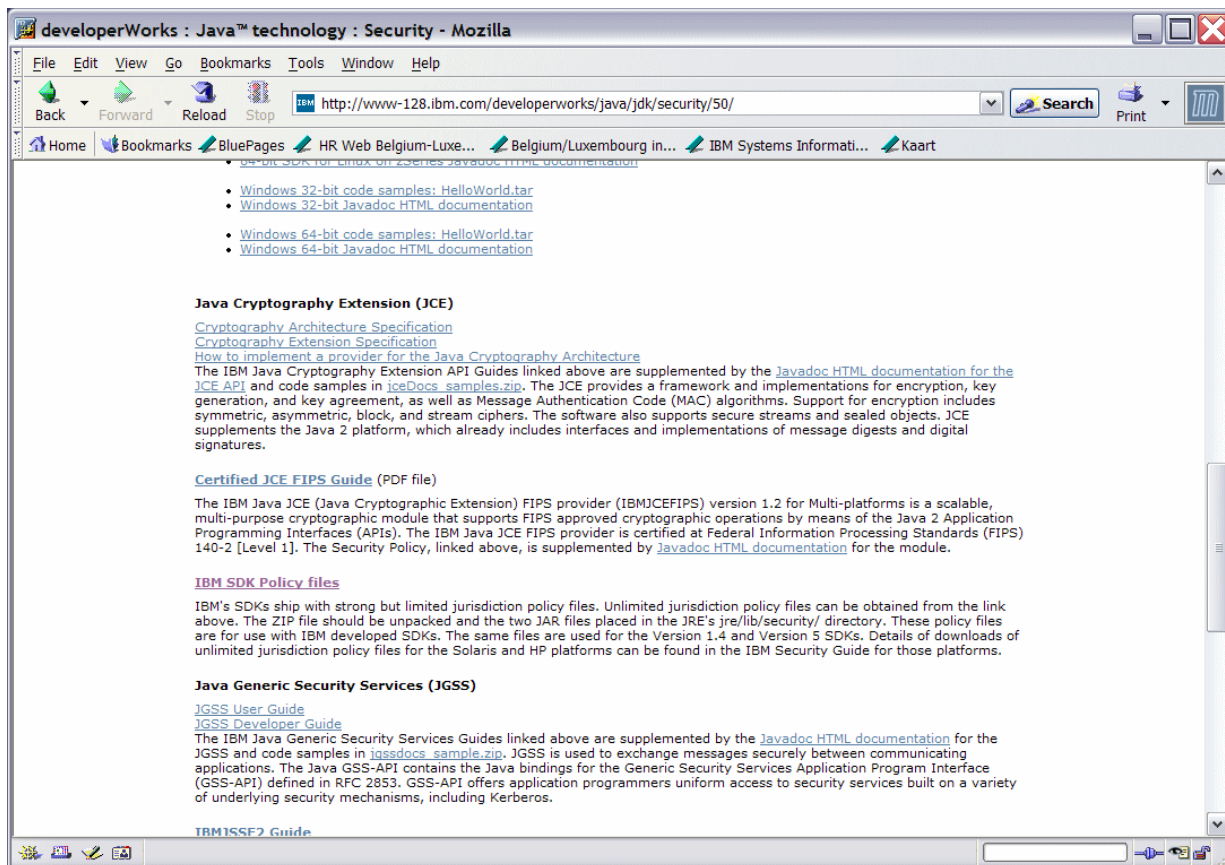


Figure 6-10 Java security site



2. Download the .zip file for V1.4.2 (Figure 6-11). The same files are used for V1.4 and V5.

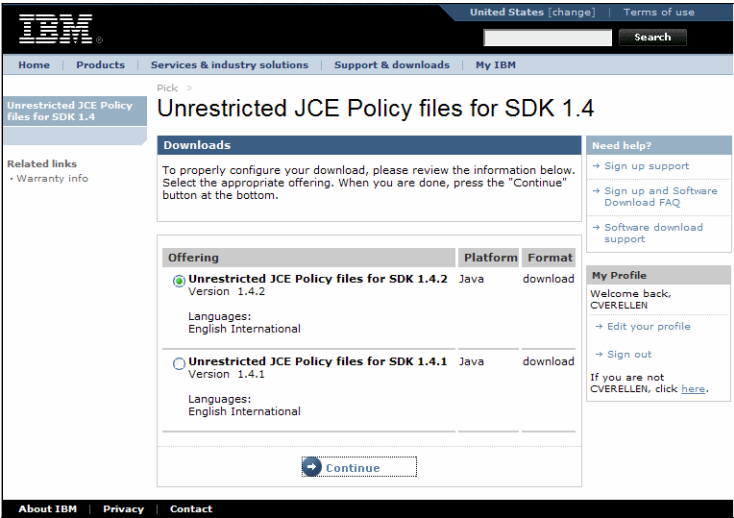


Figure 6-11 SDK version selection

3. Uncompress the .zip file to get to the two .jar files. Replace the current US\_export\_policy.jar and local\_policy.jar files in your C:\Program Files\IBM\Java50\jre\lib\security directory with the ones you just downloaded.

**Installing the Encryption Key Manager .jar and sample configuration file**

Perform the following tasks:

- 1. Download the IBM EKM Application (IBMKeyManagementServer.jar) and the IBM EKM Sample Configuration file (KeyManagerConfig.properties). Go to:  
<http://www.ibm.com/support/docview.wss?rs=1139&context=STCXRG&dc=D400&uid=ssglS4000504>

Scroll down to find the files, as shown in Figure 6-12.

DESCRIPTION	DOCUMENTATION	Download Options
Platform Multi-Platform Version Independent US English Byte Size 268588 Date 9/1/2006	<a href="#">Intro Planning &amp; User's Guide</a>	IBM EKM Application - Ver. 08232006 <a href="#">FTP</a>
Platform Multi-Platform Version Independent US English Byte Size 957 Date 9/1/2006	<a href="#">Intro Planning &amp; User's Guide</a>	IBM EKM Sample Configuration File <a href="#">FTP</a>

Figure 6-12 EKM downloads

- 2. Place the KeyManagerConfig.properties file into a directory of your choice.
- 3. Place the IBMkeyManagementServer.jar file into the directory C:\Program Files\IBM\Java50\jre\lib\ext\.

## Installing the iKeyman utility

The iKeyman utility is part of the JRE you installed. You can start it from a DOS prompt (Figure 6-13) by entering the following command:

```
cd C:\Program Files\IBM\Java50\jre\bin
java com.ibm.ikeyman.Ikeyman&
```

```
C:\>cd C:\Program Files\IBM\Java50\jre\bin
C:\Program Files\IBM\Java50\jre\bin>java com.ibm.gsk.ikeyman.Ikeyman&
_
```

Figure 6-13 Start iKeyman utility

For more details about the utility, download the *IBM Global Security Kit: Secure Sockets Layer Introduction and iKeyman User's Guide* at:

[http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/50/GSK7c\\_SSL\\_IKM\\_Guide.pdf](http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/50/GSK7c_SSL_IKM_Guide.pdf)

The standard Java tool, keytool, can also be used. Visit the Sun Java™ Web site for details about keytool usage.

### 6.1.6 Creating a keystore

To create a keystore for the encryption keys to be used by the iKeyman utility, perform the following tasks:

**Note:** In iKeyman, a keystore is called *key database* and a key is called *certificate*.

1. After entering the **java** command to start the iKeyman utility, the IBM Key Management window (Figure 6-14) is displayed. To create a new keystore, click **New**.

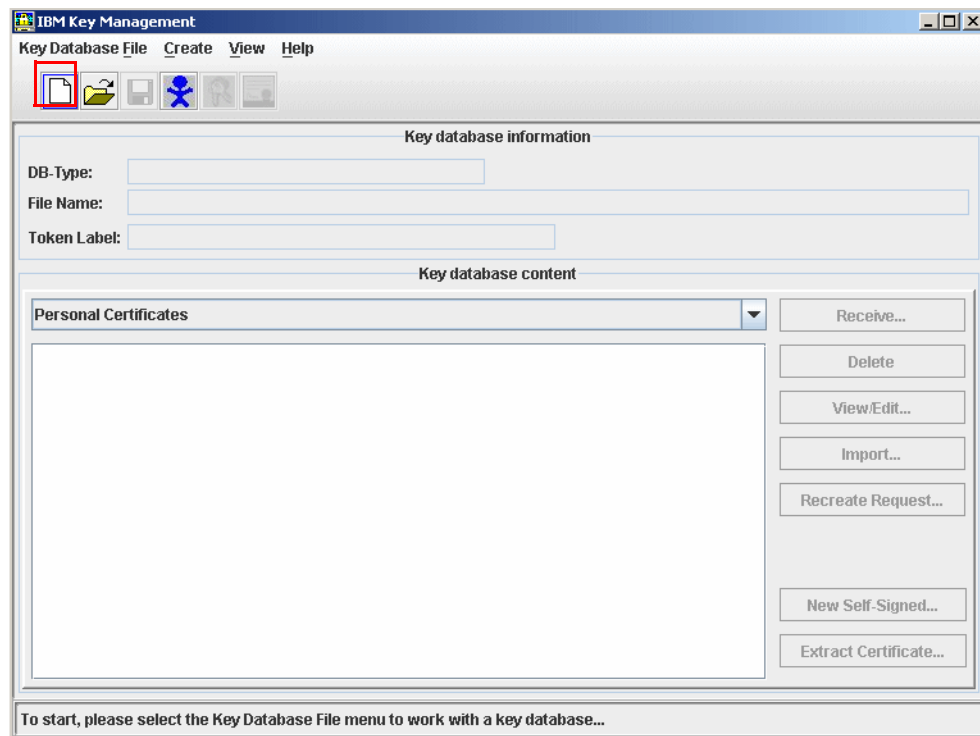


Figure 6-14 iKeyMan utility

2. The New key database window (Figure 6-15) is displayed. In this example, a JCEKS-type keystore is created. Select **JCEKS** against the Key database type field. Enter the relevant details in the File Name and Location fields. The file will be created with the name you specify here. Make sure the extension of the file is .jks. In this example, we create a keystore called keystore\_x.jks in the C:\EKM folder. Click **OK**.

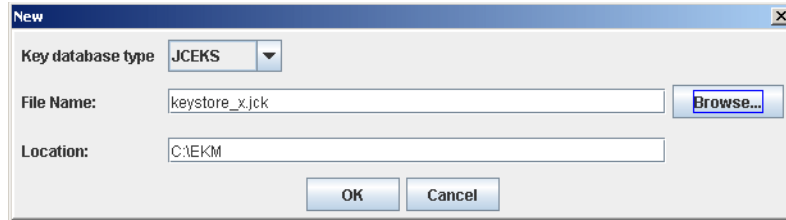


Figure 6-15 Creating keystore

3. The Password Prompt window (Figure 6-16) is displayed. Specify a password to protect the keystore. (You will need this password later to access the keystore.) Click **OK**.

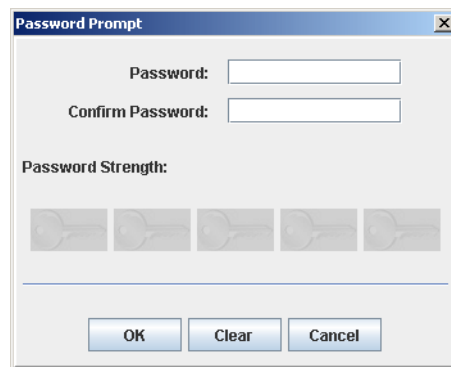


Figure 6-16 Password prompt

This completes the keystore creation. You must see the name of the keystore in the IBM Key Management window, as shown in Figure 6-17.

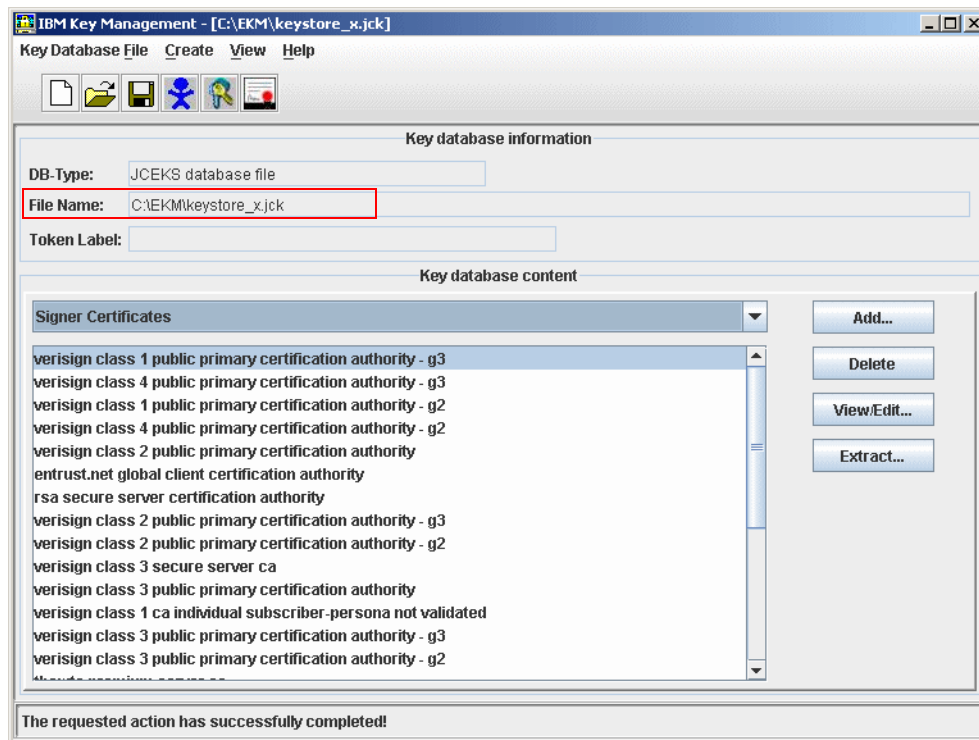


Figure 6-17 Keystore created

## 6.2 Creating keys in your keystore

This section describes how to create and move your keys into the keystore.

### 6.2.1 Creating a self-signed key

Perform the following tasks:

1. In the IBM Key Management window, click the **Create Certificate** icon on top of the page, which is highlighted in Figure 6-18.

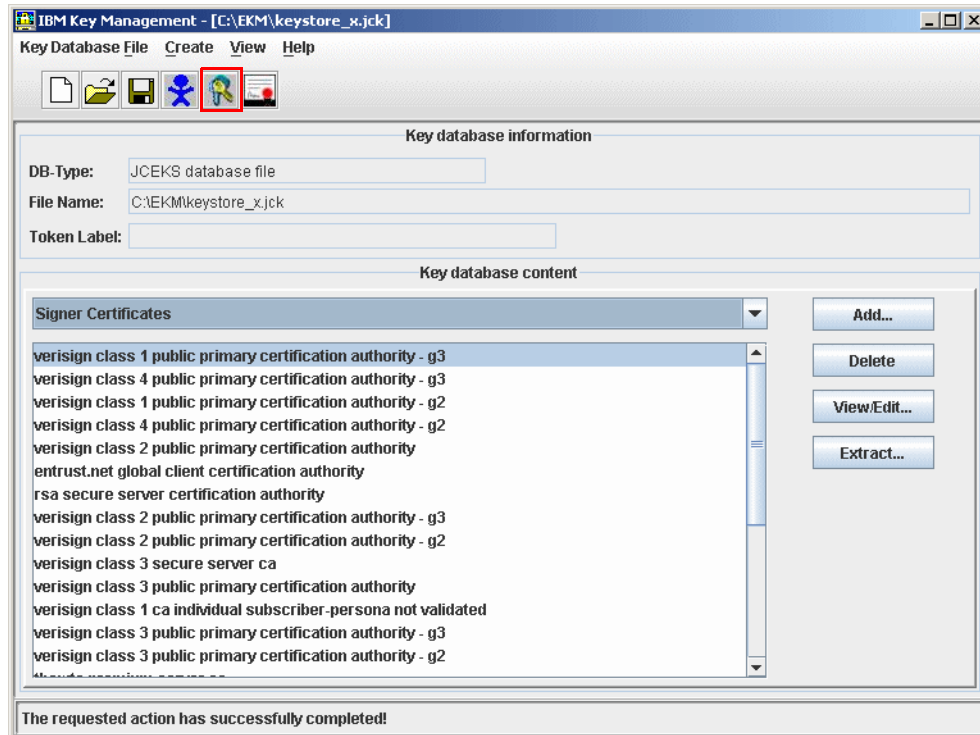
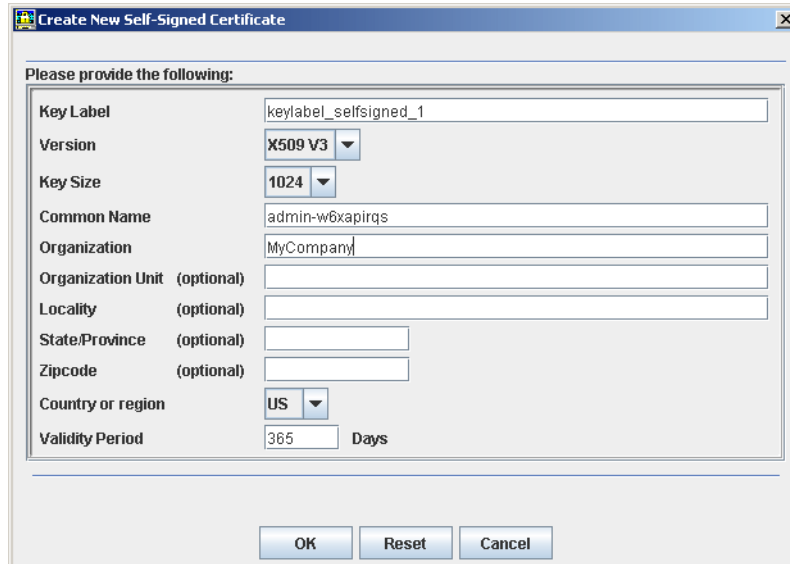


Figure 6-18 Creating self-signed key

2. The Create New Self-Signed Certificate window (Figure 6-19) opens. Specify a Key Label of your choice, but make sure that it does not contain any blanks. Select **X509 V3** from the Version menu, and **1024** from the Key Size menu. The Common Name field defaults to the computer name, but you can change it. Specify a value in the Organization field. Verify the Country or region and Validity Period fields. All other fields are optional. Click **OK**.



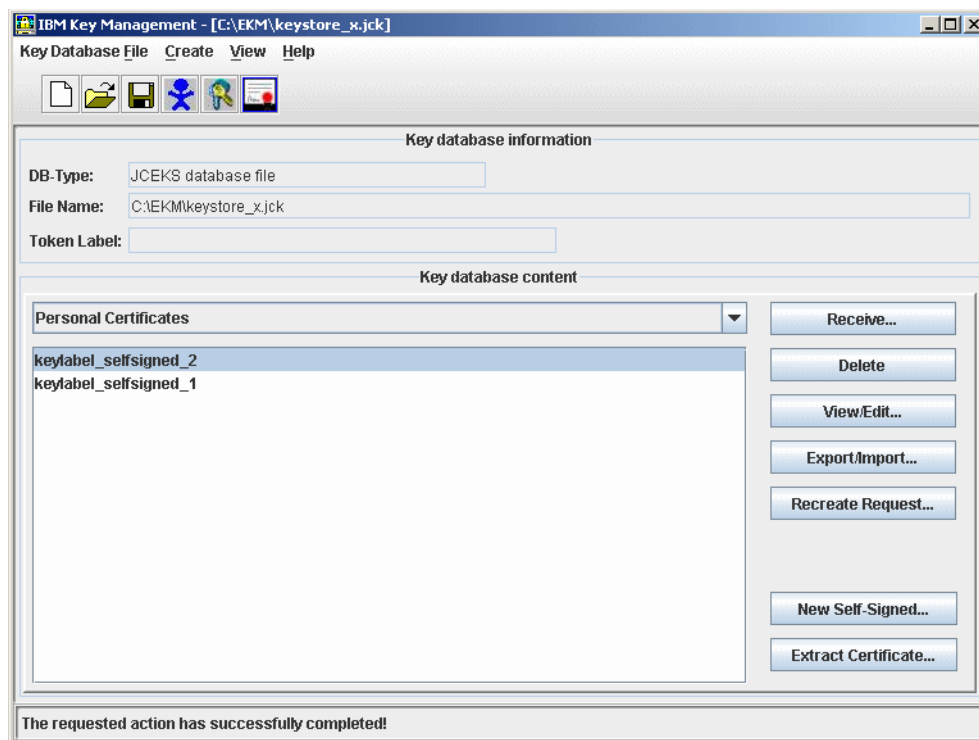
The dialog box titled "Create New Self-Signed Certificate" contains the following fields and options:

- Key Label:** keylabel\_selfsigned\_1
- Version:** X509 V3 (dropdown)
- Key Size:** 1024 (dropdown)
- Common Name:** admin-w6xapirqs
- Organization:** MyCompany
- Organization Unit (optional):** (empty)
- Locality (optional):** (empty)
- State/Province (optional):** (empty)
- Zipcode (optional):** (empty)
- Country or region:** US (dropdown)
- Validity Period:** 365 Days

Buttons at the bottom: OK, Reset, Cancel.

Figure 6-19 Creating self-signed key window

3. The key labels for the keys you create are displayed in the IBM Key Management window. In this example, we created two keys, as shown in Figure 6-20.



The IBM Key Management window shows the following information:

- Key database information:**
  - DB-Type: JCEKS database file
  - File Name: C:\EKM\keystore\_x.jck
  - Token Label: (empty)
- Key database content:**
  - Personal Certificates (dropdown menu)
  - keylabel\_selfsigned\_2
  - keylabel\_selfsigned\_1
- Actions:**
  - Receive...
  - Delete
  - View/Edit...
  - Export/Import...
  - Recreate Request...
  - New Self-Signed...
  - Extract Certificate...

Status bar: The requested action has successfully completed!

Figure 6-20 Self-signed key created

## 6.2.2 Creating a certificate request

This procedure explains how to request a certificate from a Certificate Authority (CA). A CA is a trusted third party. After you have created your certificate request, the CA signs it. The signed certificate is then held in your keystore. Follow these steps:

1. In the IBM Key Manager window, click the **Create new key and certificate request** icon on top of the page, shown highlighted in Figure 6-21.

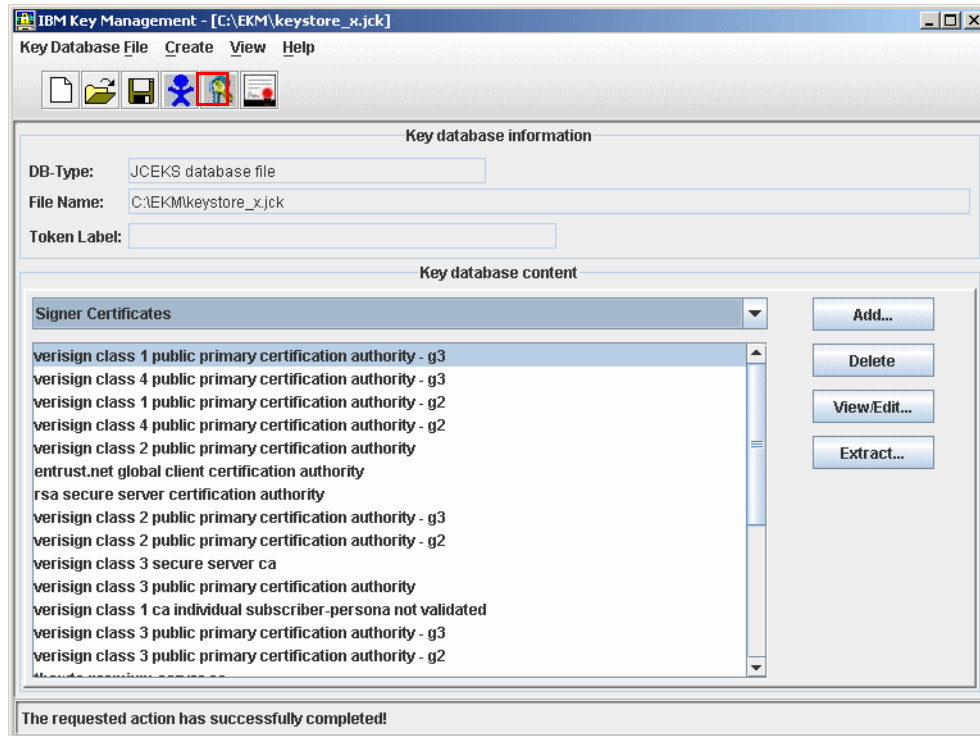
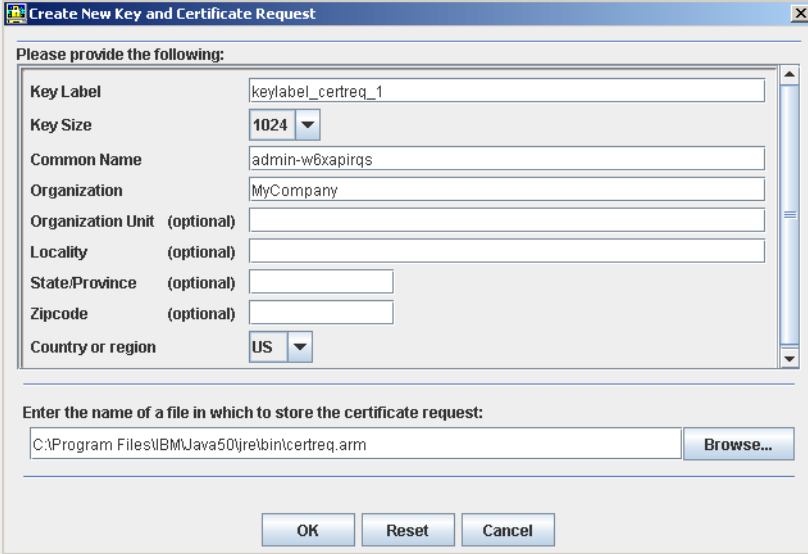


Figure 6-21 Creating new key and certificate request

2. The Create New Key and Create Certificate Request opens (Figure 6-22). Specify a Key Label of your choice that does not contain any blanks. Select **1024** from the Key Size menu. The Common Name field defaults to the computer name, but you can change it. Specify a value in the Organization field. Verify the Country or region. You can change the path and file name where the certificate request is stored. All other fields are optional.

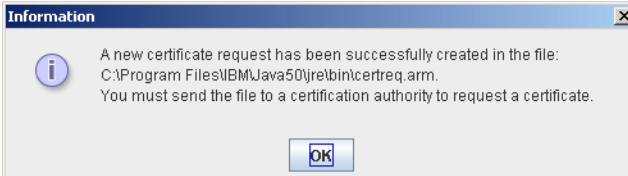


The dialog box titled "Create New Key and Certificate Request" contains the following fields and controls:

- Please provide the following:**
  - Key Label:** Text field containing "keylabel\_certreq\_1".
  - Key Size:** Dropdown menu set to "1024".
  - Common Name:** Text field containing "admin-w6xapirqs".
  - Organization:** Text field containing "MyCompany".
  - Organization Unit (optional):** Empty text field.
  - Locality (optional):** Empty text field.
  - State/Province (optional):** Empty text field.
  - Zipcode (optional):** Empty text field.
  - Country or region:** Dropdown menu set to "US".
- Enter the name of a file in which to store the certificate request:**
  - Text field containing "C:\Program Files\IBM\Java50\jre\bin\certreq.arm".
  - Browse...** button.
- Buttons:** "OK", "Reset", and "Cancel".

Figure 6-22 Create New Key and Certificate Request window

3. An Information window opens (Figure 6-23), which mentions that you must send the certificate request to a CA. Click **OK**. The CA then provides you with a signed certificate.



The "Information" dialog box displays the following message:

A new certificate request has been successfully created in the file:  
C:\Program Files\IBM\Java50\jre\bin\certreq.arm.  
You must send the file to a certification authority to request a certificate.

**OK**

Figure 6-23 Information dialog box



4. The IBM Key Management window shows the key labels for the certificate requests you create. In this example, we created two certificate requests, as shown in Figure 6-24.

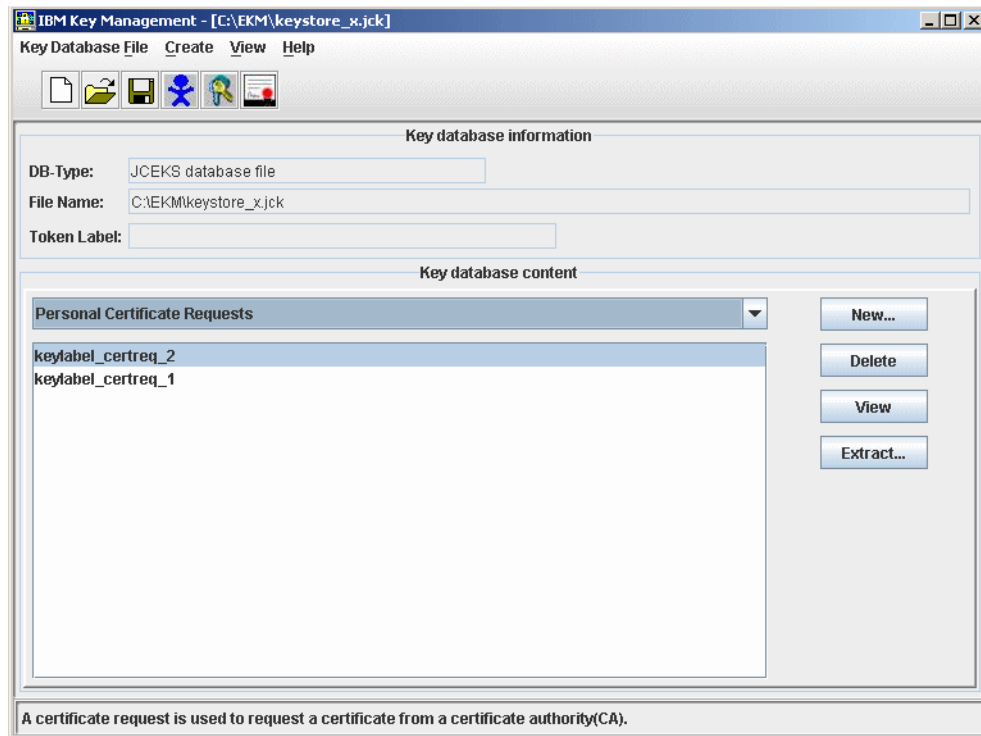


Figure 6-24 Certificate request created

### 6.2.3 Importing keys from another keystore

This section explains how to import keys from another keystore, iKeyman instance, or import a signed certificate from a CA. Follow these steps:

1. In the IBM Key Manager window (Figure 6-25), select **Personal Certificates** from the Key database content field and click **Export/Import**.

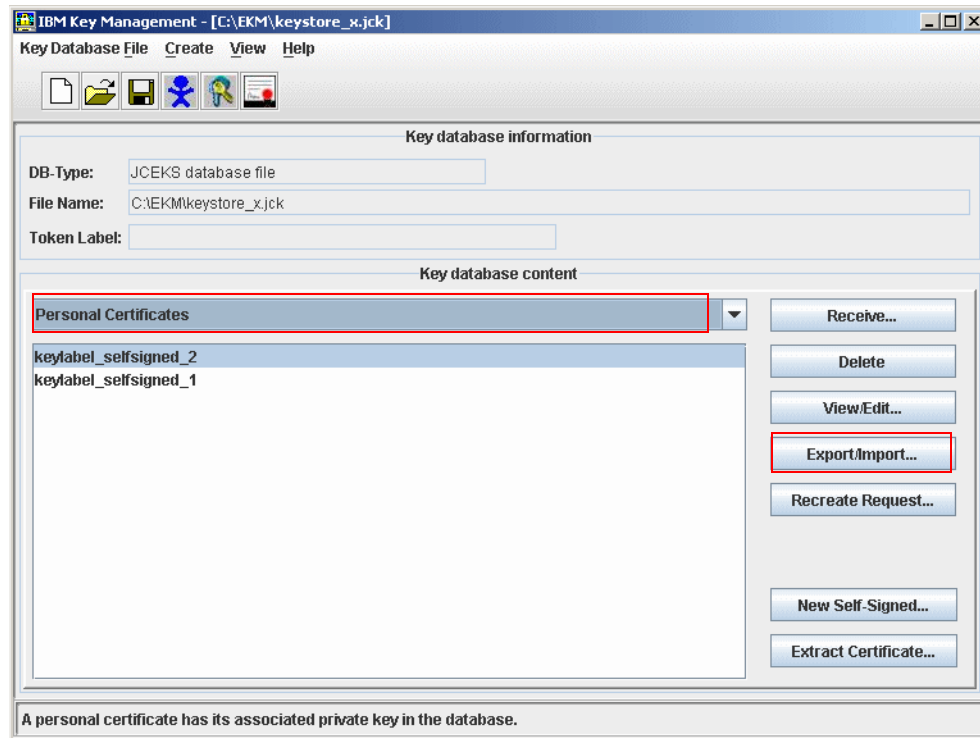


Figure 6-25 Selecting the Export/Import keys option

2. In the Export/Import window (Figure 6-26), select **Import Key** and specify the key file (that is, the keystore type, **JCEKS**), the File Name, and the Location of the keystore from which you want to import the keys. Click **OK**.

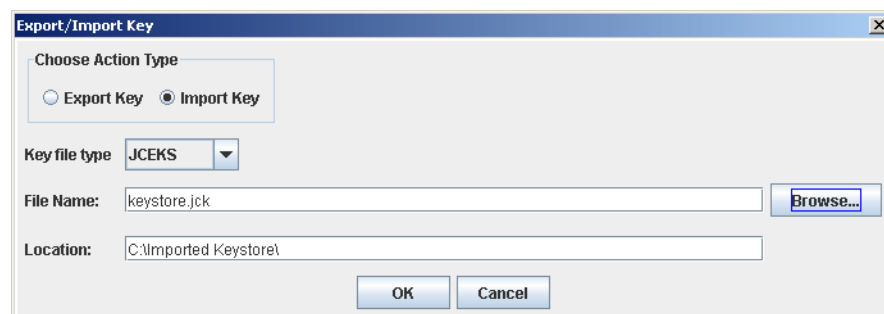


Figure 6-26 Export/Import Key dialog box

3. Authenticate to the keystore from which you want to import the keys by entering the password (Figure 6-27). Click **OK**.

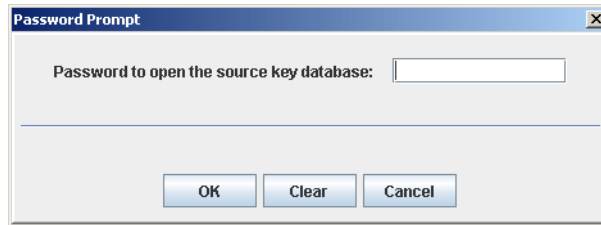


Figure 6-27 Password Prompt

4. The Select from Key Label List window (Figure 6-28) opens, listing the key labels for all of the keys stored in the keystore. Select the key labels you want to import and click **OK**.

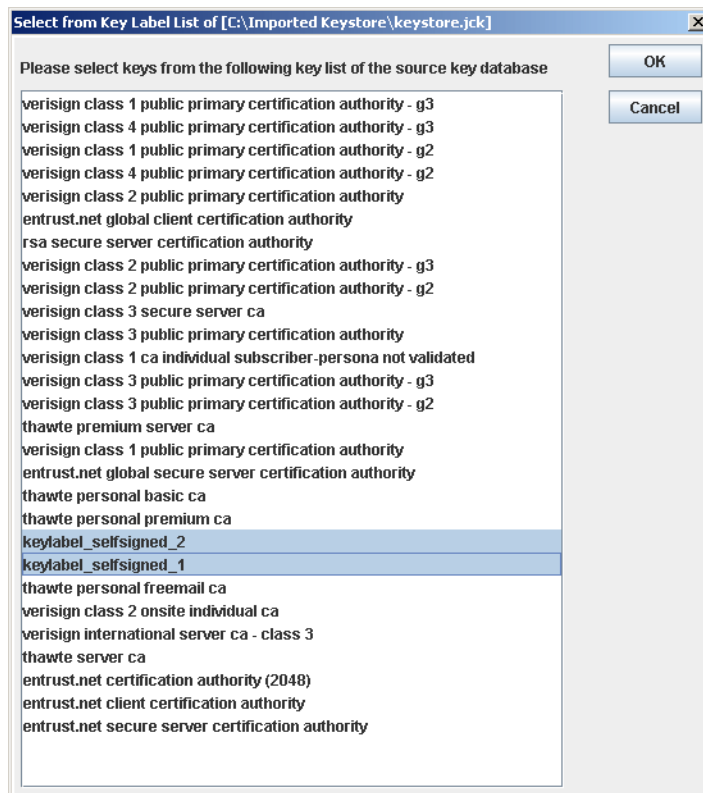


Figure 6-28 Selecting key label

5. If any of the key labels for the keys that are being imported already exists in the keystore, a Duplicate Key Label warning will be displayed (Figure 6-29). Note that the iKeyman import function has added an asterisk (\*) to the duplicate key label name in order to ensure that you do not overwrite the keys by accident. You can either accept the name change (by clicking **OK**), or edit the key label yourself (by clicking **Clear**).



Figure 6-29 Duplicate Key Label dialog box

6. Regardless of the duplicate key labels, you are always provided with the opportunity to change the key labels before you import the keys. Select the key label you want to change, enter the new name, and click **Apply**, as shown in Figure 6-30.

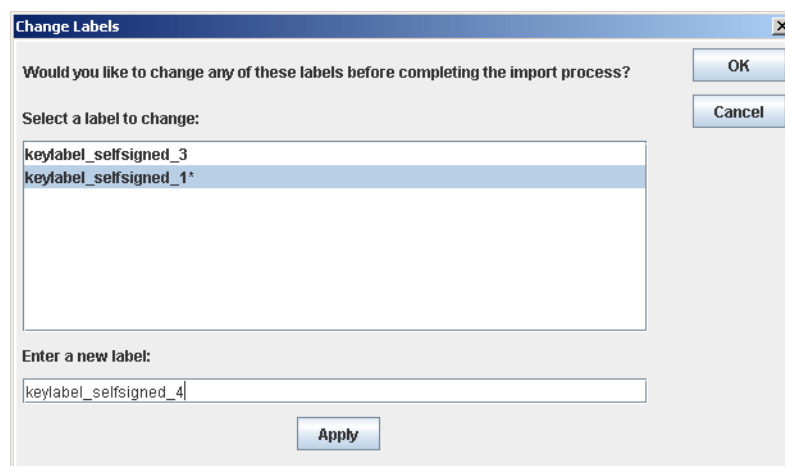


Figure 6-30 Change Labels window

7. The change is reflected in the Select area, as shown in Figure 6-31. Click **OK**.

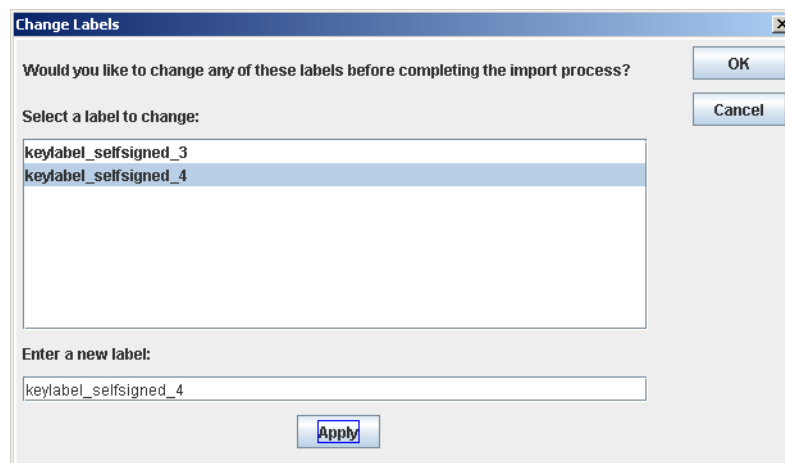


Figure 6-31 Applying label change

8. The imported keys are now displayed in your keystore in the IBM Key Manager window, as shown in Figure 6-32.

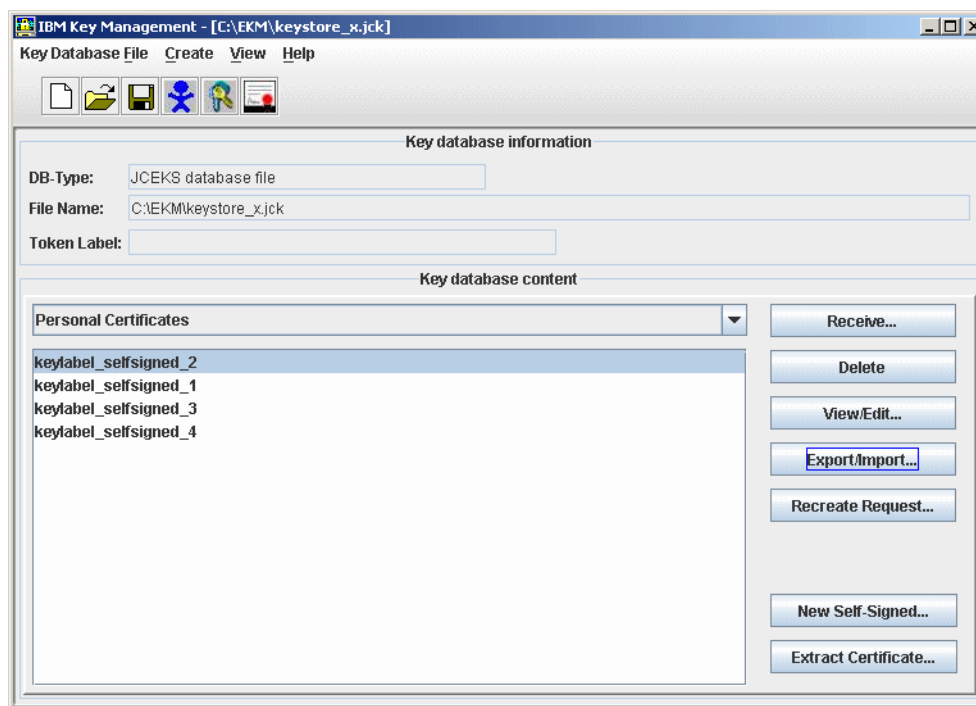


Figure 6-32 Keys are imported

## 6.3 Configuring Encryption Key Manager

Now, define to the EKM server. This is where the keys and the information on the tape drives are stored. The KeyManagerConfig.properties file is only a sample configuration. Adapt it to point the EKM server to the keystore you created, and the drive table file.

### 6.3.1 Editing the .properties file

Perform the following tasks:

1. Open the KeyManagerConfig.properties file. Choose **Select the program from a list**, as shown in Figure 6-33. Click **OK**.

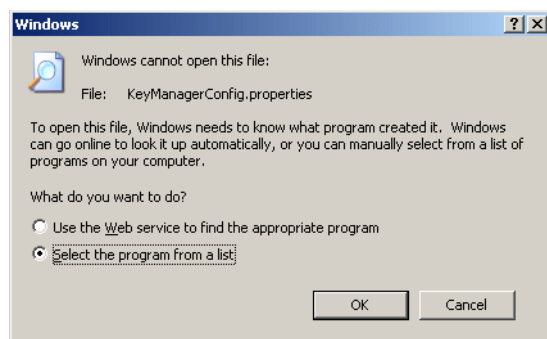


Figure 6-33 Selecting the program prompt

2. Use a text editor such as Notepad to edit the file (Figure 6-34). Click **OK**.

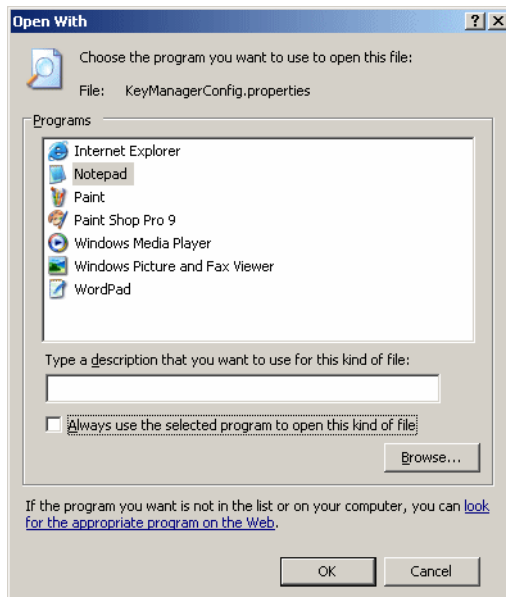


Figure 6-34 Open With window

3. Figure 6-35 on page 161 shows the sample configuration file with the default values. Some of the values must be changed and some must be added. Strictly respect the syntax, and do not leave any trailing blanks. Do not use “\” in path names; they are interpreted by Java as escape characters. Use “/” instead.
  - `Audit.handler.file.directory`  
Specify where you want EKM to store the audit log. This directory must exist before you start the EKM Admin console.
  - `Admin.ssl.keystore.name`  
`Admin.ssl.truststore.name`  
`TransportListener.ssl.keystore.name`  
`TransportListener.ssl.truststore.name`  
`config.keystore.file`  
Specify the path and the file name of the keystore.
  - `Admin.ssl.keystore.password`  
`Admin.ssl.truststore.password`  
`TransportListener.ssl.keystore.password`  
`TransportListener.ssl.truststore.password`  
`config.keystore.password`  
Specify the keystore password. You do not have to specify the password, but if you do not, you will be asked to enter it when you start the EKM server.
  - `Config.drivetable.file.url`  
Specify the path and the file name where you want EKM to store the information on the drives that are known to EKM. The path must exist before starting the EKM Admin console. You can select the file name yourself. It must have a .txt extension. It will be created by the EKM. The file path must be preceded by `FILE://`.
  - `debug.output.file`  
Specify the path and the file name of the debug file you want to create. The file must have an extension of .log.

- TransportListener.tcp.timeout  
Specify 120 (that is, the number in minutes).
- drive.acceptUnknownDrives

Set this property to true if you want the EKM server to automatically add tape drives to the EKM drive table when they contact EKM. If you decide against allowing tape drives to be added automatically, in which case you must add the tape drives manually, set this value to false. (See 6.3.4, “Adding tape drives to the EKM drive table” on page 163.)

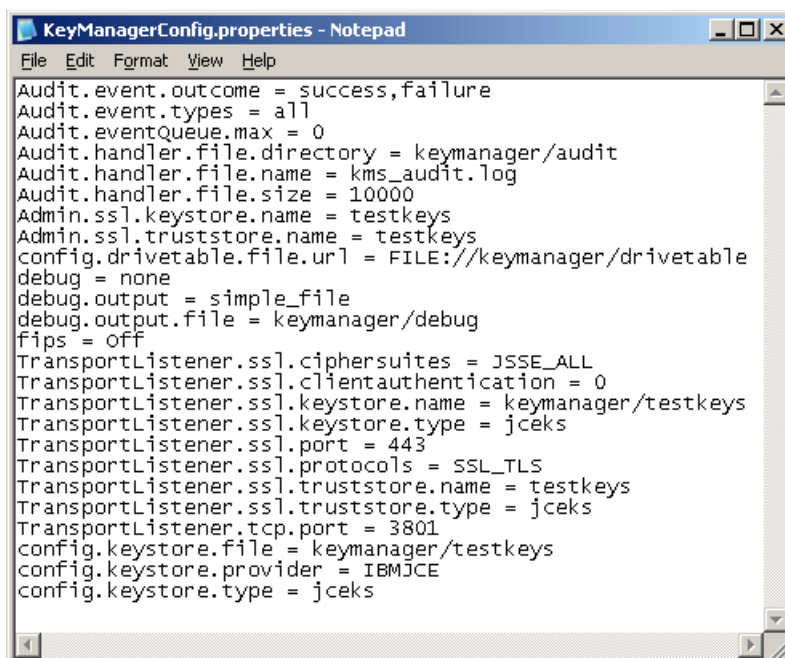


Figure 6-35 Default properties

Figure 6-36 shows the KeyManagerConfig.properties file with the correct values for the configuration in this example.

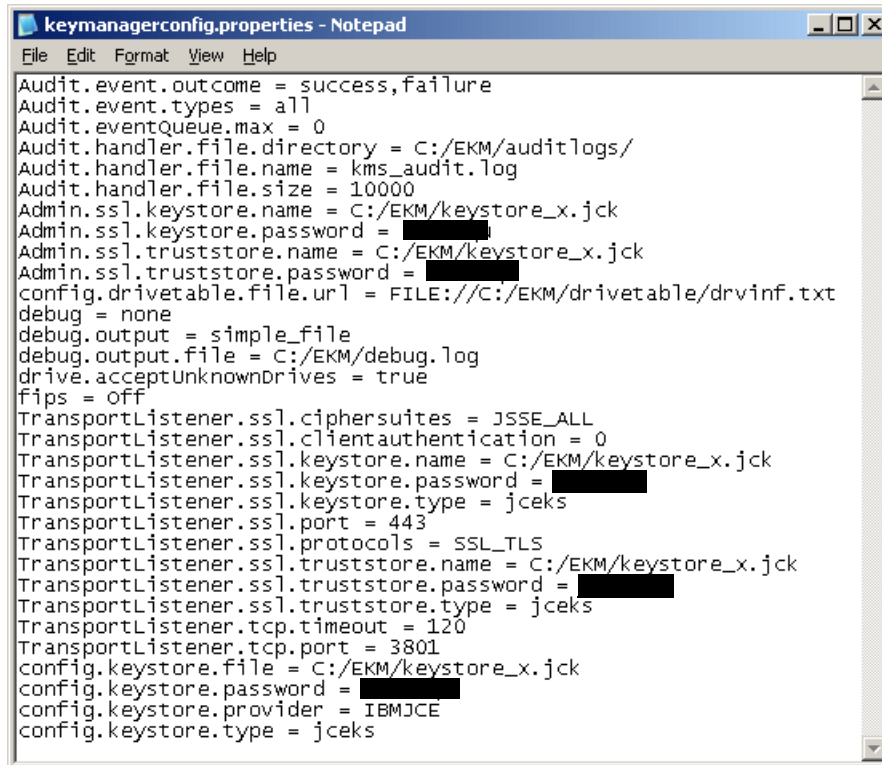


Figure 6-36 Changed properties

4. Save the changes to the KeyManagerConfig.properties file.

### 6.3.2 Starting the EKM Admin Console (command prompt)

Do not modify the KeyManagerConfig.properties file when the EKM Admin console is running because the changes will be lost. If you want to make changes, end the EKM Admin console first, and restart it after you have made the changes. The properties file is read only at startup and the values are stored in memory. When the EKM Admin console is ended, it writes the values in memory to the KeyManagerConfig.properties file in case any changes were made using the EKM commands when the admin/server is up. For information about EKM commands, refer to *IBM Encryption Key Manager component for the Java platform, EKM Introduction, Planning, and User's Guide*, GA76-0418-00.

Enter the following commands from a DOS prompt to start the EKM Admin console:

```
cd C:/Program Files/IBM/Java50/jre/bin
java com.ibm.keymanager.KMSAdminCmd KeyManagerConfig_full_file_path_name
```

**Note:** The path name for the KeyManagerConfig.properties file must not contain blanks.

After the command has been entered the DOS # prompt is displayed and you can continue to type in the relevant EKM console command.



### 6.3.3 Starting and stopping the EKM server

To start the EKM server, enter `startekm` at the prompt. To stop it, enter `stopekm` (Example 6-1).

*Example 6-1 Starting the EKM Admin console and the EKM server*

---

```
C:\Program Files\IBM\Java50\jre\bin>java com.ibm.keymanager.KMSAdminCmd
C:/EKM/keymanagerco
nfig.properties
# startekm
Loaded drive key store successfully
Starting the Encryption Key Manager 1.0
Processing Arguments
Processing
Server is started
# stopekm
Stopping the EKM admin service...
#
```

---

### 6.3.4 Adding tape drives to the EKM drive table

If you decide against allowing tape drives to be added automatically, specify `drive.acceptUnknownDrives = false`, but in that case, you must add the tape drives manually before using EKM.

Start the EKM Admin console and enter the following command from the command prompt for each drive:

```
adddrive -drivename drivename -rec1 alias1 -rec2 alias2
```

*drivename* is the serial number of the drive (for example, *000001365054*). The serial number must comprise 12 characters. Use leading zeroes.

`-rec1` and `-rec2` are optional parameters. They are the default keys assigned to your drive in the event that the key requested for use with a cartridge loaded in your drive is not present in the keystore.

**adddrive** is only one of the available EKM commands. For more information about EKM commands, refer to *IBM Encryption Key Manager component for the Java platform, EKM Introduction, Planning, and User's Guide*, GA76-0418.

## 6.4 Encryption Key Manager on i5/OS

This section describes the installation requirements and implementation steps involved in running an EKM on i5/OS.

### 6.4.1 Software requirements

Table 6-2 shows the minimum i5/OS versions and their corresponding minimum SDK versions.

Table 6-2 Supported i5/OS versions and their corresponding SDK versions

i5/OS	IBM SDK	Licensed program feature codes and PTF level
V5R3	IBM Developer Kit for Java - Java Developer Kit 5.0	<ul style="list-style-type: none"><li>▶ 5722JV1 *BASE and option 7</li><li>▶ The latest Java group PTF SF99269<sup>a</sup></li><li>▶ PTF SI25093 for 5722SS1 Option 3 (Extended base directory support)</li><li>▶ 5722AC3 (Cryptographic Access Provider)</li></ul>
V5R4	IBM Developer Kit for Java - Java 2 Platform, Standard Edition (J2SE™) 5.0 32-bit	<ul style="list-style-type: none"><li>▶ 5722JV1 *BASE and Option 8</li><li>▶ Install SR3 or SR2 for J2SE 5.0:<ul style="list-style-type: none"><li>– SR3: PTF number is not yet available at the time of publication</li><li>– SR2: PTF SI24375 for 5722JV1</li></ul></li><li>▶ The latest Java group PTF SF99291<sup>a</sup></li><li>▶ PTF SI25094 for 5722SS1 Option 3 (Extended base directory support)</li><li>▶ Cryptographic Access Provider is included in the base in V5R4</li></ul>

a. For the latest level, refer to the following Web site:

[http://www-912.ibm.com/s\\_dir/sline003.NSF/GroupPTFs?OpenView&view=GroupPTFs](http://www-912.ibm.com/s_dir/sline003.NSF/GroupPTFs?OpenView&view=GroupPTFs)

After you have the required operating system, SDK (JDK™ or J2SE), and the PTFs installed, as shown in Table 6-2:

- ▶ Install the IBM Java unrestricted policy files (refer to 6.4.2, “Installing the unrestricted policy files” on page 164)
- ▶ Install the IBM EKM Application and the IBM EKM Sample Configuration file (see 6.4.3, “Installing the Encryption Key Manager .jar and sample configuration file” on page 165)
- ▶ Install the proper tool to manage the keys in your type of keystore. In this example, we defined an IBMi5OSkeystore-type keystore. The interface to manage this type of keystore is the Digital Certificate Manager (DCM) GUI (refer to 6.4.4, “Installing Digital Certificate Manager” on page 165). The iKeyman utility enables you to create the JCEKS keystore type (refer to Installing the iKeyman utility in 6.1.5, “Encryption Key Manager server on a PC” on page 142).

### 6.4.2 Installing the unrestricted policy files

There are two ways in which to get the unrestricted policy files:

- ▶ Downloading the unrestricted policy files from the IBM Web site (refer to “Installing the unrestricted policy files” on page 146) and placing the files in the /QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit/jre/lib/security/ directory in the Installable File System (IFS).

- Installing the unrestricted policy files through a PTF.
  - For i5/OS V5R3, install SI24671 for 5722JV1
  - For i5/OS V5R4, install SI24672 for 5722JV1, and then copy the unrestricted policy files from /qibm/proddata/java400/jdk15/lib/security/ to /QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit/jre/lib/security/

### 6.4.3 Installing the Encryption Key Manager .jar and sample configuration file

For i5/OS V5R3, install PTF SI25093 for 5722SS1. This PTF installs the EKM code, the default configuration properties file, and the script file.

For i5/OS V5R4, perform the following tasks:

1. Install PTF SI25094 for 5722SS1. This PTF installs the default configuration properties file and the script file.
2. If J2SE V5.0 SR2 is installed (PTF SI24375), download the IBMKeyManagementServer.jar file from the IBM TotalStorage site (refer to the TS1120 topic). Go to:

<http://www.ibm.com/servers/storage/support/tape/ts1120/downloading.html>

Click **Downloadable files**. On the page that is displayed, select **IBM Encryption Key Manager component for the Java Platform**. Scroll down to find the file, as shown in Figure 6-37 and place it in the /QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit/jre/lib/ext/ directory.

DESCRIPTION	DOCUMENTATION	Download Options
Platform Multi-Platform Version Independent US English Byte Size 268588 Date 9/1/2006	<a href="#">Intro Planning &amp; User's Guide</a>	IBM EKM Application - Ver. 08232006 <a href="#">FTP</a>
Platform Multi-Platform Version Independent US English Byte Size 957 Date 9/1/2006	<a href="#">Intro Planning &amp; User's Guide</a>	IBM EKM Sample Configuration File <a href="#">FTP</a>

Figure 6-37 EKM downloads

When SR3 becomes available, it contains the EKM code. Therefore, you do not have to download the IBMKeyManagementServer.jar file.

### 6.4.4 Installing Digital Certificate Manager

In this example, we define an IBMi5OSkeystore-type keystore. The interface to manage this type of keystore is the DCM GUI. The iKeyman utility enables you to create the JCEKS keystore type ("Installing the iKeyman utility" on page 148). Perform the following tasks:

1. Verify that these licensed programs are installed on your system. If not, install them first:
  - 5722SS1 option 34: DCM
  - 5722DG1: IBM Hypertext Protocol Server (HTTP) Server for i5/OS
2. Open iSeries Navigator and select on your system.

3. Select **Network** → **Servers** → **TCP/IP** and check in the right pane to see whether the HTTP Administration server is started. If not, right-click **HTTP Administration** to start it (Figure 6-38).

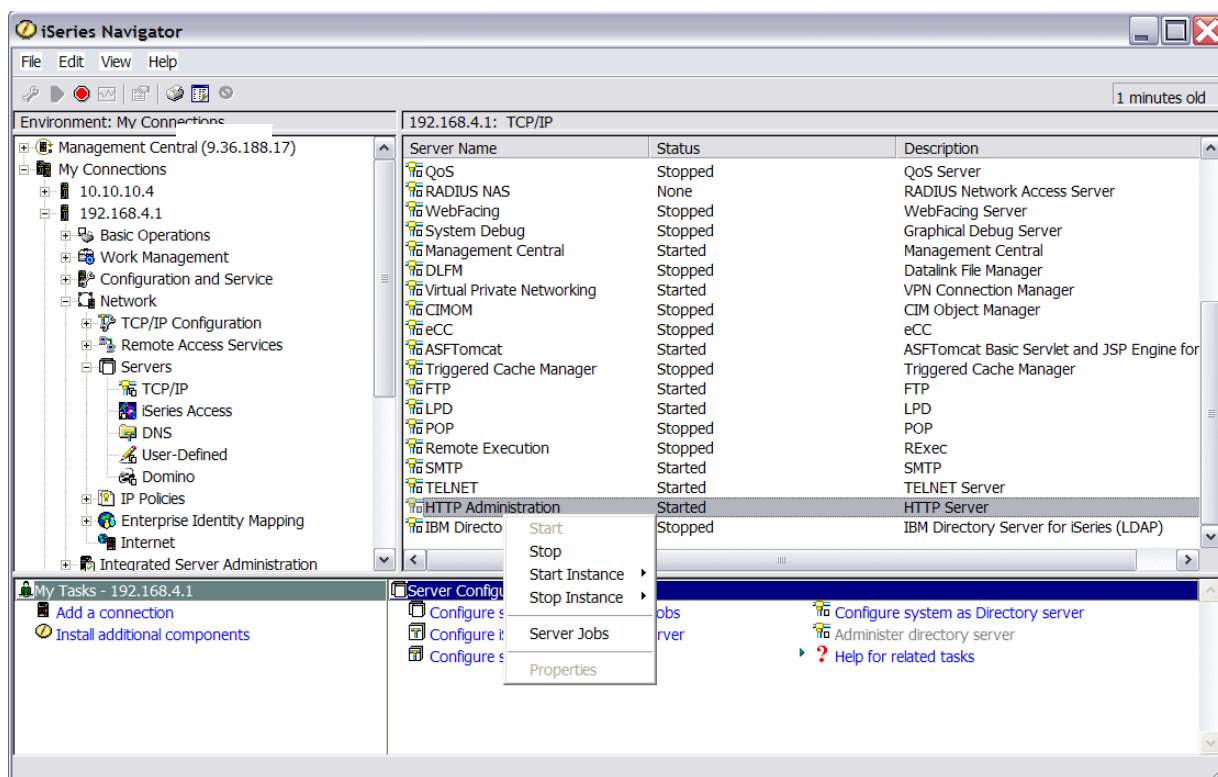


Figure 6-38 Starting HTTP Administration server

4. In a Web browser, go to:  
http://IP address:2001

5. The i5/OS Tasks window is shown. Select **Digital Certificate Manager** (Figure 6-39).



Figure 6-39 i5/OS Tasks window

This takes you to the DCM start page (Figure 6-40 on page 168). The installation is complete.

## 6.5 Creating a keystore in DCM

This section shows you how to create the certificate store in DCM and how to move the keys into the store.

**Note:** In DCM, a keystore is called *certificate store* and a key is called a *certificate*.

To create a keystore, perform the following tasks:

1. From the DCM start page (Figure 6-40), select **Create New Certificate Store**.

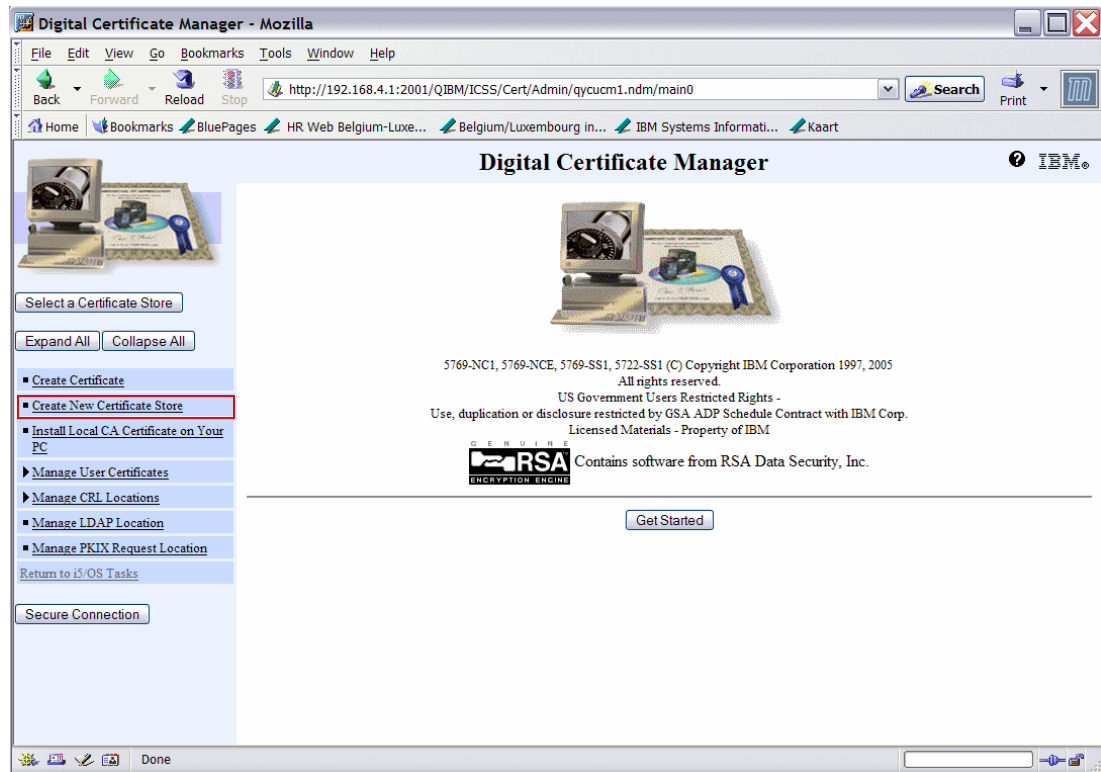


Figure 6-40 DCM start page

2. In the Create New Certificate Store window, select **Other System Certificate Store** and click **Continue**, as shown in Figure 6-41.



Figure 6-41 Creating new certificate store 1

3. Select **No - Do not create a certificate in the certificate store**. Click **Continue** (Figure 6-42).



Figure 6-42 Creating new certificate store 2

4. In the Certificate Store Name and Password window (Figure 6-43), specify the Certificate store path and file name.

If the path does not exist in your System i5 environment, create it first by using the CRTDIR command. The file name can be anything but must have a .kdb extension. This file is created automatically. You must specify the same path and file name in your EKM configuration file. Specify a password for the certificate (“key”) store and click **Create**.

**Important:** The keystore is now in a user directory of the i5/OS IFS. Be careful *not* to back up the keystore to the encrypted tapes, because you will not be able to recover the keys, and without the keys you cannot access any of the data on your encrypted tapes. There is *no recovery* from lost keys.



Figure 6-43 Certificate Store name and password

The Certificate Store Created window opens (Figure 6-44 on page 170). Your keystore is created successfully.

## 6.5.1 Creating keys

To create your keys, generate them with DCM.

### Accessing the keystore to generate keys

Perform the following tasks:

1. Choose **Select a Certificate Store** in the left panel of the DCM window (Figure 6-44).

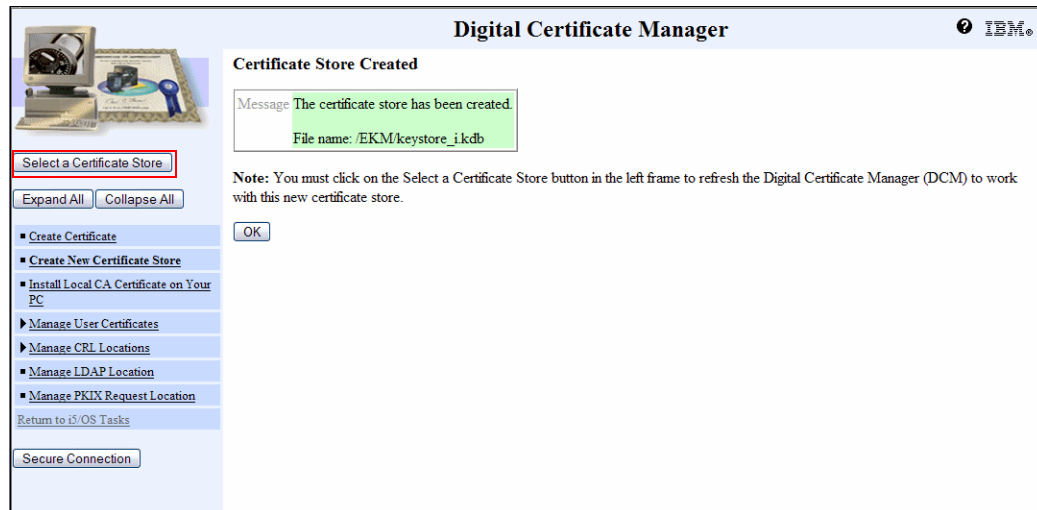


Figure 6-44 Certificate Store Created window

2. Select **Other System Certificate Store** and click **Continue** (Figure 6-45).



Figure 6-45 Select a Certificate Store window



3. In the Certificate Store and Password panel, enter the keystore file name you created earlier (enter the complete path name) and the password as shown in Figure 6-46, and click **Continue**.

The screenshot shows the 'Digital Certificate Manager' window with the 'Certificate Store and Password' panel active. The panel contains the following elements:

- Select a Certificate Store** button.
- Expand All** and **Collapse All** buttons.
- A list of tasks: **Create Certificate**, **Create New Certificate Store**, **Install Local CA Certificate on Your PC**, **Manage User Certificates**, **Manage CRL Locations**, **Manage LDAP Location**, and **Manage PKIX Request Location**.
- Return to i5/OS Tasks** link.
- Secure Connection** button.
- Certificate type:** Server or client.
- Example certificate store file name:** /MYDIRECTORY/MYFILE.KDB.
- Certificate store path and filename:** /EKM/keystore\_ikdb.
- Certificate store password:** A text field with masked characters (\*\*\*\*\*).
- Continue**, **Reset Password**, and **Cancel** buttons.

Figure 6-46 Certificate Store authentication

4. The Current Certificate Store window opens (Figure 6-47). You are now “inside” the keystore you selected and can start managing it.

The screenshot shows the 'Digital Certificate Manager' window with the 'Current Certificate Store' panel active. The panel contains the following elements:

- Select a Certificate Store** button.
- Expand All** and **Collapse All** buttons.
- A list of tasks: **Fast Path**, **Create Certificate**, **Create New Certificate Store**, **Install Local CA Certificate on Your PC**, **Manage Certificates**, **Manage Certificate Store**, **Manage CRL Locations**, **Manage LDAP Location**, and **Manage PKIX Request Location**.
- Return to i5/OS Tasks** link.
- Secure Connection** button.
- Current Certificate Store** header.
- Text: You have selected to work with the certificate store listed below. The left frame is being refreshed to show the task list for this certificate store. Select a task from the left frame to begin working with this certificate store.
- Certificate type:** Server or client.
- Certificate store path and filename:** /EKM/KEYSTORE\_I.KDB.

Figure 6-47 Current Certificate Store window

There are two ways in which to work with the keystore you selected:

- In the left column, select **Fast Path** → **Work with server and client certificates** (Figure 6-48).



Figure 6-48 DCM Fast Path window

- Alternatively, select **Manage Certificates** in the left panel (Figure 6-49).



Figure 6-49 Manage Certificates window

## 6.5.2 Creating a private/public key pair in your keystore

This procedure explains how to request a certificate from a CA. A CA is a trusted third party. After you create your certificate request, the CA signs it. The signed certificate is then held in your keystore.

Perform the following tasks:

1. Click the **Create Certificate** option in the left column. In the right panel, select **Server or client certificate**, and click **Continue**, as shown in Figure 6-50.



Figure 6-50 Create Certificate window

2. Select **VeriSign or other Internet Certificate Authority (CA)** and click **Continue** (Figure 6-51).

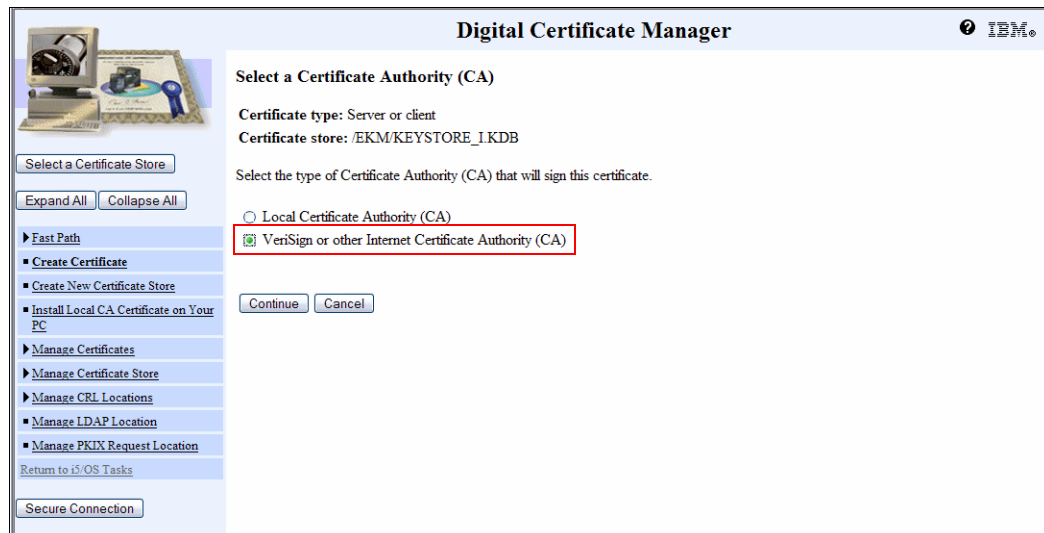




Figure 6-51 Select a Certificate Authority window

- 

## Digital Certificate Manager



### Create Certificate

**Certificate type:** Server or client

**Certificate store:** /EKM/KEYSTORE\_1.KDB

Use this form to create a certificate in the certificate store listed above.

**Key size:**  (bits)

**Certificate label:**  (required)

#### Certificate Information

**Common name:**  (required)

**Organization unit:**

**Organization name:**  (required)


**Locality or city:**

**State or province:**  (required; minimum of 3 characters)


**Country or region:**  (required)

- [Fast Path](#)
  - [Create Certificate](#)
  - [Create New Certificate Store](#)
  - [Install Local CA Certificate on Your PC](#)
  - [Manage Certificates](#)
  - [Manage Certificate Store](#)
  - [Manage CRL Locations](#)
  - [Manage LDAP Location](#)
  - [Manage PKIX Request Location](#)
  - [Return to i5/OS Tasks](#)
  - [Secure Connection](#)

*Figure 6-52 Creating a certificate*

- 

## Digital Certificate Manager

 IBM

### Certificate Request Created

The certificate request data is shown below. Copy and paste the request data, including both the Begin request and End request lines, into the form that the Certificate Authority (CA) provides.

**Warning:** If you exit this page, the certificate request data is lost. Therefore, make sure you carefully copy and paste the data into the Certificate Authority (CA) form or into a file for later use.

Select a Certificate Store

Expand All   Collapse All

- ▶ Fast Path
  - Create Certificate
  - Create New Certificate Store
  - Install Local CA Certificate on Your PC
  - ▶ Manage Certificates
  - ▶ Manage Certificate Store
  - ▶ Manage CRL Locations
  - Manage LDAP Location
  - Manage PKIX Request Location

[Return to i5/OS Tasks](#)

Secure Connection

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB3jCB9AIBADBLMQewCQYDVQQGwWJUZzEPMA0GA1UECBMTXDAxRzSMRiEwAYD
VQKKEw1NeUNvBxbHbnkxZzAVBgNVBAMTDKVLITUN1cnRpZmlzYXR1MIGFMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDjcmAKWjYC/mY2/JfPQOu2PFy+LvhSdInQ1CbvM
VwHDAI4dD/1UFTPBjGulE2fp224C14+hNbqo1B/AtCnqoGKfPq1SIdmWUvsgpziq
Hoc1jyerzDeY1W9RfciVwXXTPFYOKF4lyFo9kC0JnCtTnqoGKfPq1SIdmWUvsgpziq
Gp53MQIDAQABAAwDQYJKoZIhvcNAQEBQADYEAOCe6gFAZBgcfhD/vSWItXtXG
nnCeu6T8crxKJBXJdCkwpKYNafzj74bnYn4ANqCQWRAS19xeVRiN177Ic99Lk913
FvK/Lvc233LfyziFwkw3qY53F5LkbC0jnwYp6Xw311Qy3q9wBafscQp0c0rYmki
YPy2SACNHqUKZdLGuko=
-----END NEW CERTIFICATE REQUEST-----
```

*Figure 6-53 Certificate Request Created window*

The CA returns a signed certificate to you. Store the file on System i5, in the IFS.

### 6.5.3 Importing a key into the keystore

To import a key into the keystore, perform the following tasks:

1. Import the signed certificate into your keystore. You can use this method to import keys from another keystore. Click **Work with server and client certificates**, verify that the Certificate store is correct, and click **Import**, as shown in Figure 6-54.

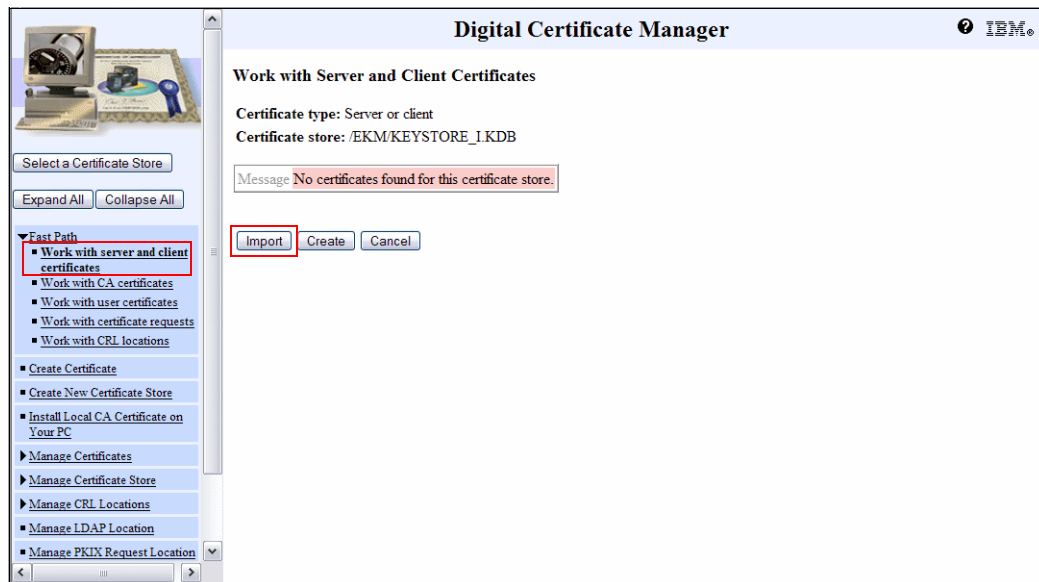


Figure 6-54 Importing the signed certificate

2. Enter the complete IFS path name of the file in which you pasted the signed certificate data and click **Continue**, as shown in Figure 6-55.

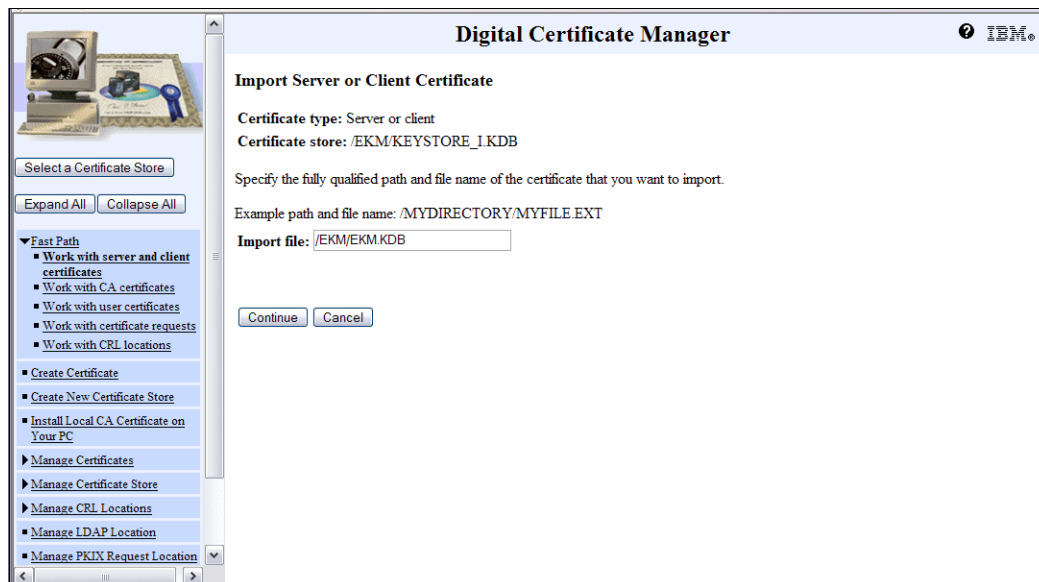


Figure 6-55 Importing the file

3. Enter the password for the keystore from which you want to import the keys, and specify the key label. Click **Continue** (Figure 6-56).

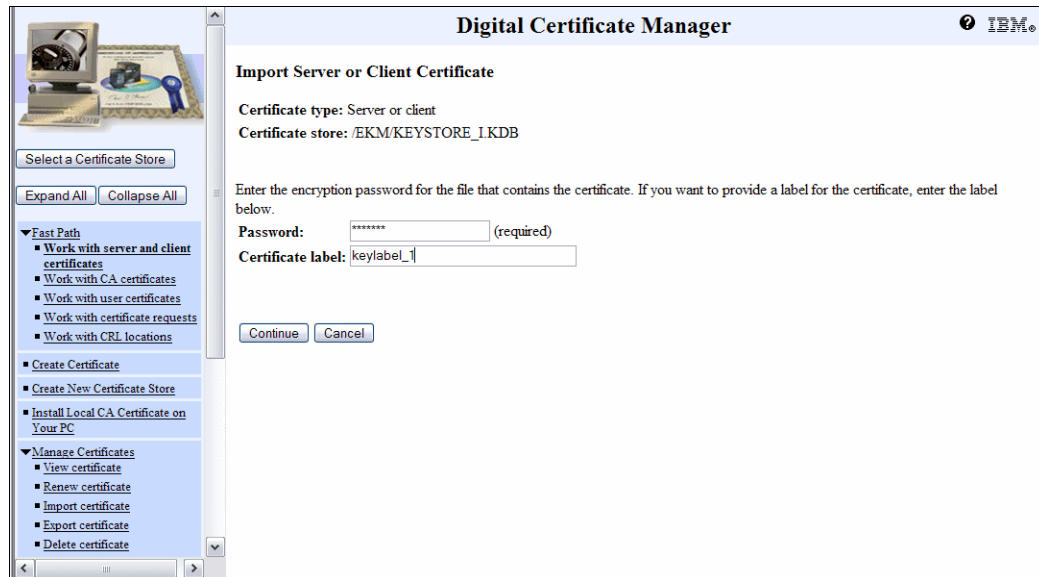


Figure 6-56 Importing the key

This key is then imported into your keystore.

#### 6.5.4 Creating a local Certificate Authority-signed key in your keystore

An alternative to the third-party CA-signed keys, if it intended *only* for internal use, is a locally signed key, also called “local CA-signed certificate.” The DCM does not create self-signed certificates as such.

Perform the following tasks:

1. Create a local CA certificate if it is not yet created. To do this, perform the following tasks:
  - a. Click **Create a Local CA Certificate**.
  - b. The Create a Certificate Authority window opens. Select a key size of **1024**.
  - c. Click **Select a Certificate Store** and select your keystore.

2. Click **Install Local CA Certificate on Your PC**. In the right panel, click **Install certificate**, as shown in Figure 6-57.



Figure 6-57 Instal Local CA Certificate on Your PC window

3. Select the **Work with Server and Client Certificates** option and click **Create**, as shown in Figure 6-58.

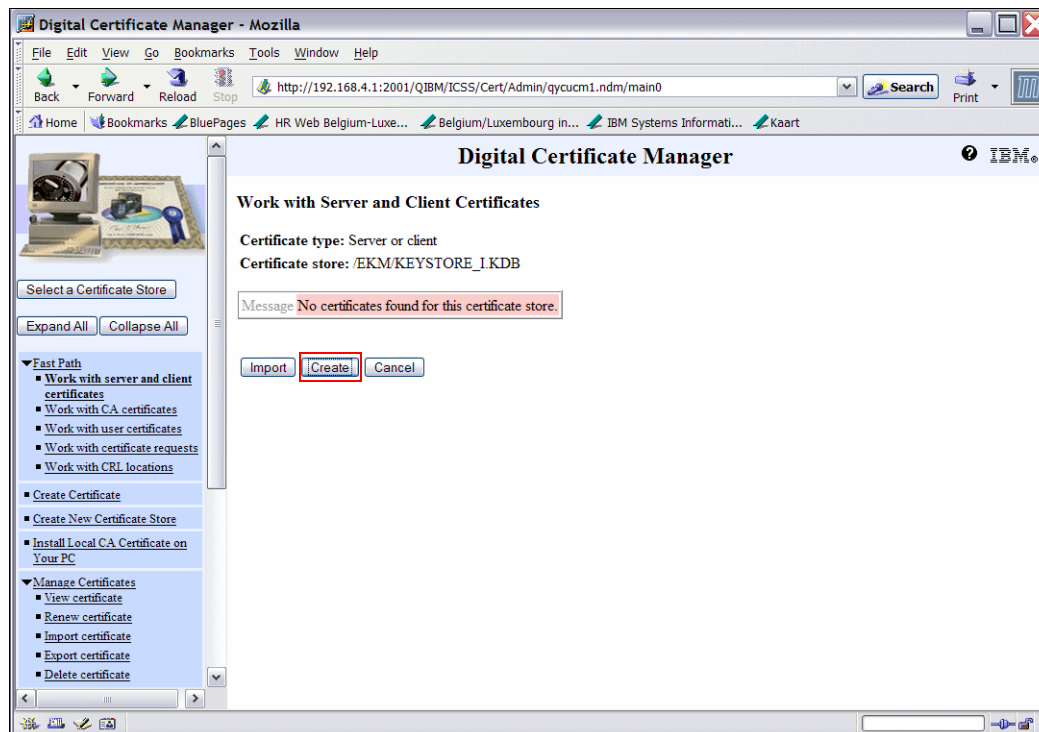


Figure 6-58 Work with Server and Client Certificates window



4. In the Select a Certificate Authority window, select **Local Certificate Authority (CA)** and click **Continue** (Figure 6-59).

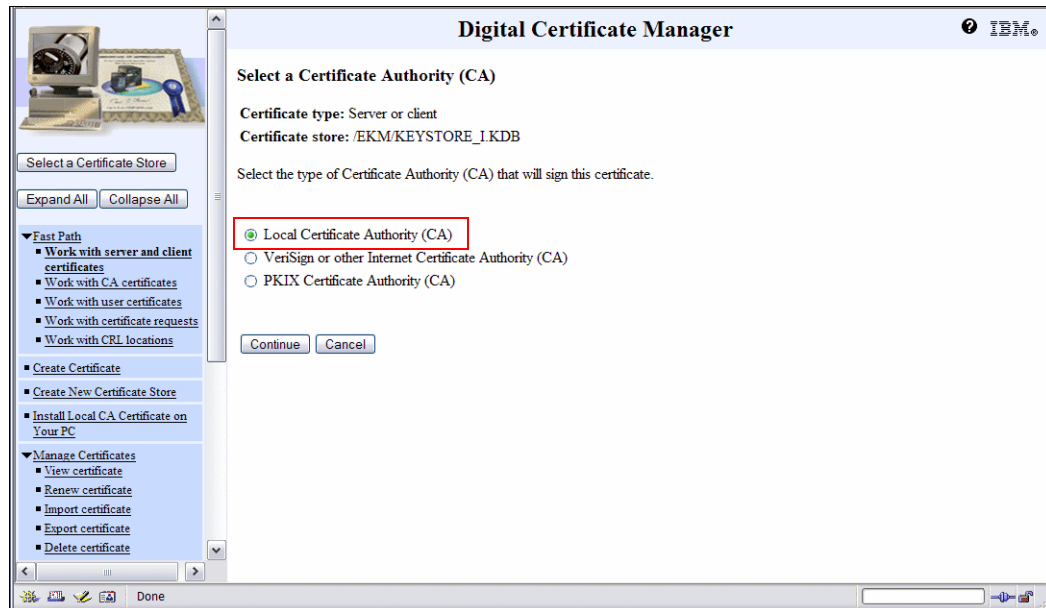


Figure 6-59 Selecting Local Certificate Authority

5. The Create Certificate window is displayed. Select a key size of **1024** and a certificate label, and complete the required fields, as shown in Figure 6-60. Click **Continue**.

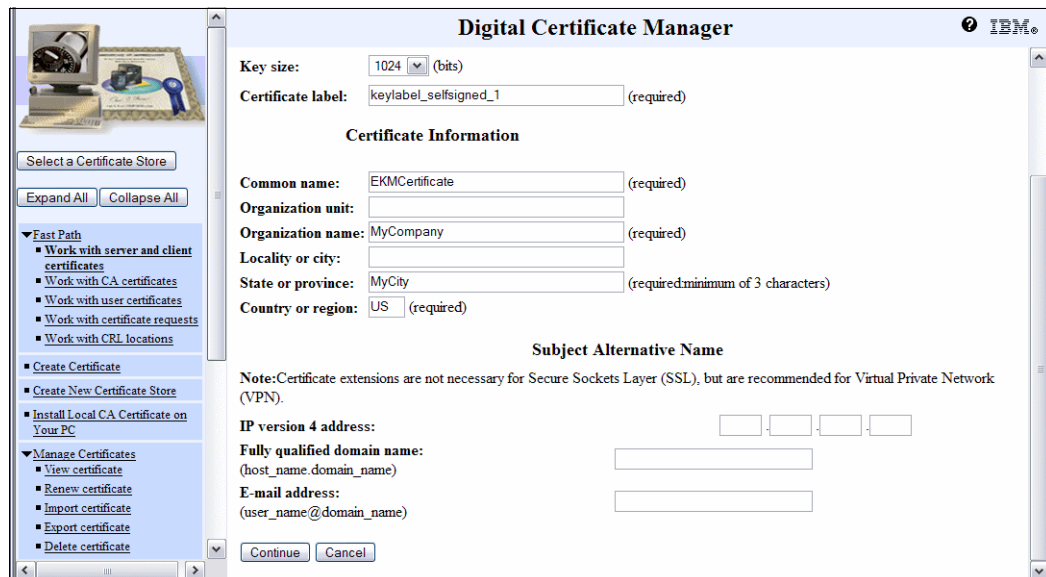


Figure 6-60 Creating the certificate



The Certificate Created Successfully window is displayed (Figure 6-61). Click **OK**.

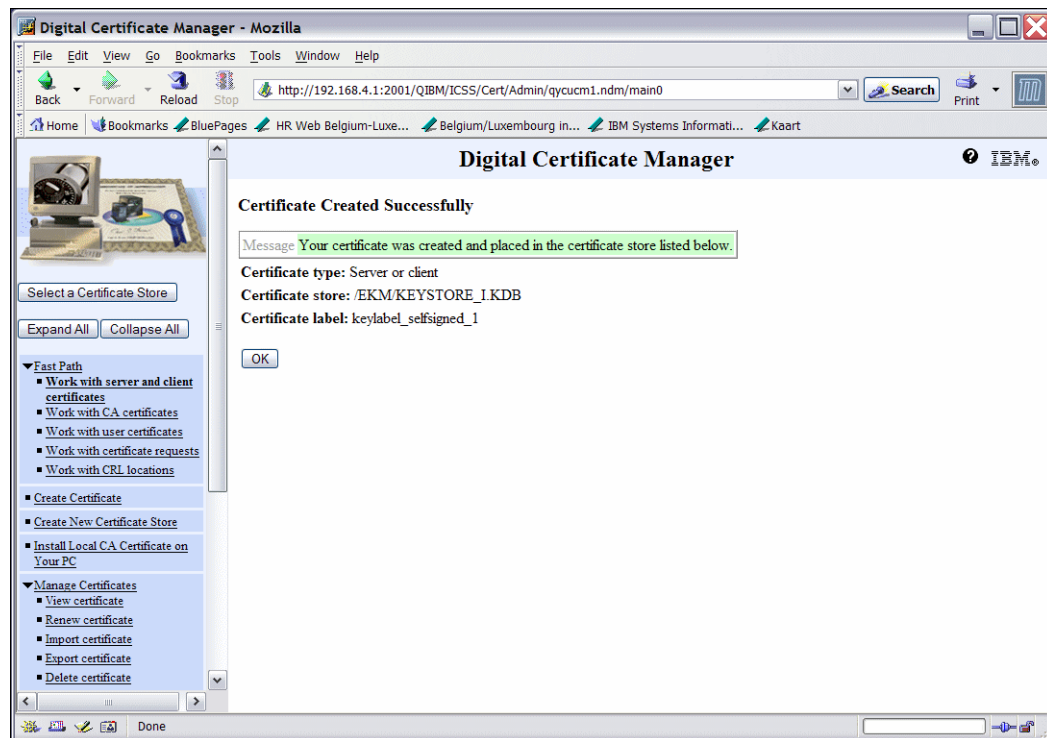


Figure 6-61 Certificate is created

## 6.6 Configuring Encryption Key Manager

Now, define to the EKM server where the keys and the information on the tape drives are stored. The KeyManagerConfig.properties file is only a sample configuration. Adapt it to point the EKM server to the keystore you created and the drive table file.

### 6.6.1 Editing the .properties file

Perform the following tasks to edit the .properties file:

1. From an i5/OS command line, type the WRKLNK command and go down to the KeyManagerConfig.properties file. Type 2 to edit the file, as shown in Figure 6-62.

```
Work with Object Links

Directory . . . . : /EKM

Type options, press Enter.
  2=Edit   3=Copy   4=Remove   5=Display   7=Rename   8=Display attributes
  11=Change current directory ...

Opt  Object link          Type   Attribute   Text
---  ---
    keystore_i.kdb        STMF
    keystore_i.RDB        STMF
    EKM.KDB               STMF
    EKM.RDB               STMF
  2_  KeyManagerConfig.p > STMF

Parameters or command
====>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F12=Cancel   F17=Position to
F22=Display entire field   F23=More options

Bottom
```

Figure 6-62 Edit .properties file

2. Figure 6-63 on page 181 shows the sample configuration file with the default values. Change some of the values and add some. Strictly respect the syntax and do not leave any trailing blanks. Do not use “\” in path names. They are interpreted by Java as escape characters. Use “/” instead.
  - Audit.handler.file.directory  
Specify where you want EKM to store the audit log. This directory must exist before you start the EKM Admin console.
  - Admin.ssl.keystore.name  
Admin.ssl.truststore.name  
TransportListener.ssl.keystore.name  
TransportListener.ssl.truststore.name  
config.keystore.file  
Specify the path and the file name of the keystore.
  - Admin.ssl.keystore.password  
Admin.ssl.truststore.password  
TransportListener.ssl.keystore.password  
TransportListener.ssl.truststore.password  
config.keystore.password

Specify the keystore password. You do not have to specify the password, but if you do not do it, you will be asked to enter it when you start the EKM server.

- `Config.drivetable.file.url`

Specify the path and the file name where you want EKM to store the information on the drives that are known to EKM. The path must exist before starting the EKM Admin console. You can choose the file name yourself but it must have a .txt extension. It will be created by the EKM. The file path must be preceded by `FILE://`.

- `debug.output.file`

Specify the path and the file name of the debug file you want to create. The file must have a .log extension.

- `drive.acceptUnknownDrives`

Set this property to true if you want the EKM server to automatically add the tape drives to the EKM drive table when they contact EKM. If you decide against allowing the tape drives to be added automatically, which means that you will have to add the tape drives manually, set this value to false. (Refer to 6.6.4, “Adding the tape drives to the EKM drive table” on page 183.)

```
Edit File: /EKM/KeyManagerConfig.properties
Record : 1 of 49 by 10      Column : 1 76 by 126
Control : _____

CMD .....1.....2.....3.....4.....5.....6.....7.....8.....9.....0.....1.....2...
*****Beginning of data*****
# Note that the file is sorted by property name. EKM shutdown automatically
# reorders the values in the properties file.
Audit.event.outcome = success,failure
Audit.event.types = all
Audit.eventQueue.max = 0
# Need to change the following directory value or create the directories
Audit.handler.file.directory = /EKM/auditlogs
Audit.handler.file.name = ekm_audit.log
Audit.handler.file.size = 10000
# Need to change the following 2 pathnames to the correct pathnames for
# the keystores being used on your system
Admin.ssl.keystore.name = /EKM/EKM.kdb
Admin.ssl.truststore.name = /EKM/EKM.kdb
# Need to change the following pathname value or create the directories
config.drivetable.file.url = FILE:///EKM/drives/drivetable
# Need to change the following pathname to the correct pathname for
# the keystore being used on your system

F2=Save F3=Save/Exit F12=Exit F15=Services F16=Repeat find F17=Repeat change F19=Left F20=Right
```

Figure 6-63 Sample .properties file

3. Save the changes to the KeyManagerConfig.properties file.

## 6.6.2 Starting the EKM Admin Console (command prompt)

This section describes how to start the EKM admin console from the QShell command line.

**Important:** Do not modify the KeyManagerConfig.properties file when the EKM Admin console is running. The changes will be lost. If you want to make changes, end the EKM Admin console first, and restart it after you have made the changes. The properties file is only read at startup and the values are stored in memory. When the EKM Admin console is ended, it writes the values in memory to the KeyManagerConfig.properties file in case any changes are made using the EKM commands when the admin/server is up. For information about EKM commands, refer to *IBM Encryption Key Manager component for the Java platform, EKM Introduction, Planning, and User's Guide*, GA76-0418.

Perform the following tasks:

1. To start the EKM Admin console, enter the STRQSH command on an i5/OS command line.
2. Start the EKM Admin console from the QSH command line by entering:  
`strEKM -propfile fully_qualified_properties_file_name`
3. The screen shown in Figure 6-64 opens. To show Help on the strEKM script, type:  
`strEKM -h`

```

QSH Command Entry

$

===> strEKM -propfile /EKM/KeyManagerConfig.properties_

```

---

```

F3=Exit  F6=Print F9=Retrieve F12=Disconnect
F13=Clear F17=Top  F18=Bottom F21=CL command entry

```

Figure 6-64 QSH Command Entry screen

4. When the EKM Admin server is started, the # prompt is available, as shown in Figure 6-65.

```

QSH Command Entry

$
> strEKM -propfile /EKM/KeyManagerConfig.properties
Sep 7, 2006 11:29:06 AM com.ibm.keymanger.config.ConfigImpl get
FINER: ENTRY
Sep 7, 2006 11:29:06 AM com.ibm.keymanger.config.ConfigImpl get
ALL: debug.output = simple_file
Sep 7, 2006 11:29:06 AM com.ibm.keymanger.config.ConfigImpl get
FINER: RETURN
#

===> 

```

---

```

F3=Exit  F6=Print F9=Retrieve F12=Disconnect
F13=Clear F17=Top  F18=Bottom F21=CL command entry

```

Figure 6-65 Start EKM Admin Console

### 6.6.3 Starting and stopping the EKM server

To start the EKM server, enter the following command from the QSH command entry (Figure 6-66):

```
strEKM -server -propfile fully_qualified_properties_file_name
```

To stop the EKM server, enter:

```
stopEKM
```

You can also run the server in a batch job. In that case, end the batch job to stop the server.

```
QSH Command Entry

$
> strEKM -server -propfile /EKM/KeyManagerConfig.properties
Sep 7, 2006 11:41:01 AM com.ibm.keymanger.config.ConfigImpl get
FINER: ENTRY
Sep 7, 2006 11:41:01 AM com.ibm.keymanger.config.ConfigImpl get
ALL: debug.output = simple_file
Sep 7, 2006 11:41:01 AM com.ibm.keymanger.config.ConfigImpl get
FINER: RETURN
# Loaded drive key store successfully
Starting the Encryption Key Manager 1.0-20060823
Processing Arguments
Processing
Server is started
#

===> _

F3=Exit F6=Print F9=Retrieve F12=Disconnect
F13=Clear F17=Top F18=Bottom F21=CL command entry
```

Figure 6-66 Starting the EKM server

### 6.6.4 Adding the tape drives to the EKM drive table

If you decide against allowing the tape drives to be added automatically, specify:

```
drive.acceptUnknownDrives = false
```

In such a situation, you add the tape drives manually before using EKM.

To add the tape drives to the EKM drive table, start the EKM Admin console and enter the following command from the # prompt for each drive:

```
addrdrive -drivename drivename -rec1 alias1 -rec2 alias2
```

*drivename* is the serial number of the drive (for example, 000001365054). Note that the serial number must comprise 12 characters. Use leading zeroes.

-rec1 and -rec2 are the optional parameters. They are the default keys assigned to your drive in the event that the key requested for use with a cartridge loaded in your drive is not present in the keystore.

**addrdrive** is only one of the available EKM commands. For more information about EKM commands, refer to *IBM Encryption Key Manager component for the Java platform, EKM Introduction, Planning, and User's Guide*, GA76-0418.

## 6.7 Configuring your TS1120 tape drive for encryption

This section describes how to configure your TS1120 tape drive for encryption using the TS3500 Tape Library Specialist Web interface.

### 6.7.1 Defining the keystores to be used by the TS3500

To enable encryption, point the TS3500 tape library to where it can find the keystore or the “Key Manager” you created. When the TS1120 tape drive located in the library wants to write or read an encrypted tape, it requests keys from the keystore. All you have to do is point the tape library system to the key manager by adding its address:

1. Go to the IBM System Storage™ Tape Library Specialist Web interface (Figure 6-67). For instructions for setting up the IBM System Storage Tape Library Specialist Web interface, refer to *IBM System Storage TS3500 Tape Library: Operator Guide*, GA32-0560-01.

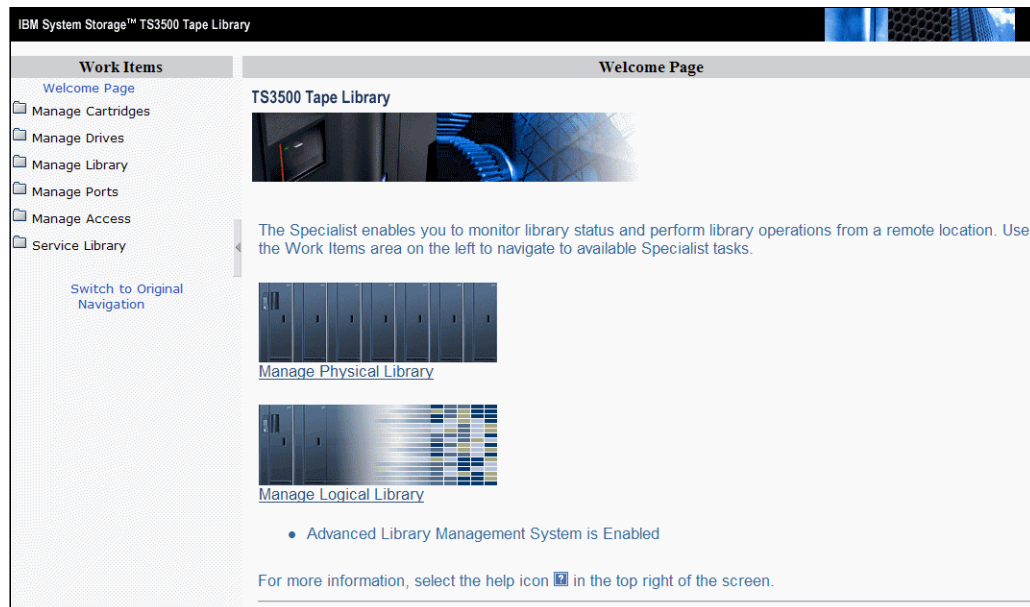


Figure 6-67 IBM System Storage Tape Library Specialist Web interface

2. In the left panel of the tape library Web interface, select **Manage Access** → **Key Manager Addresses**, as shown in Figure 6-68.

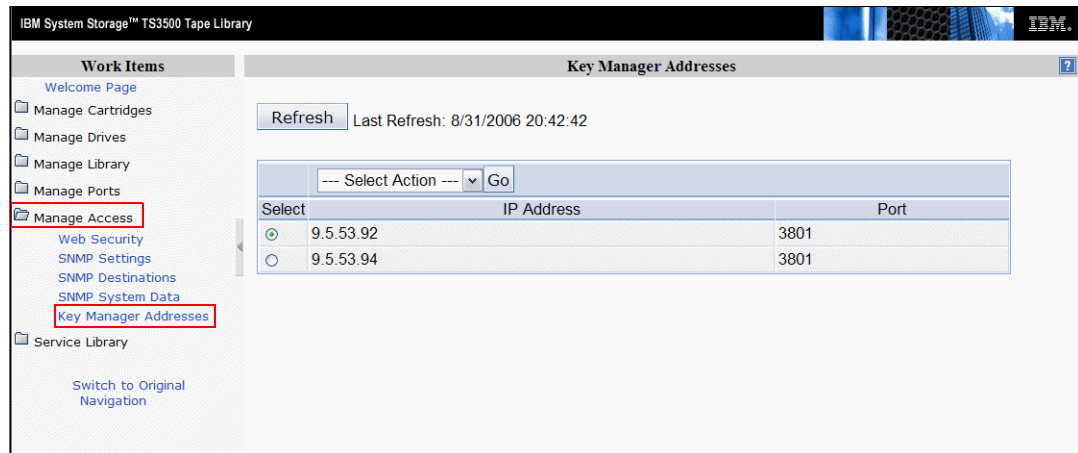


Figure 6-68 Key Manager Addresses

3. To add a key manager address, select **Create** in the Select Action menu, and click **Go** (Figure 6-69).

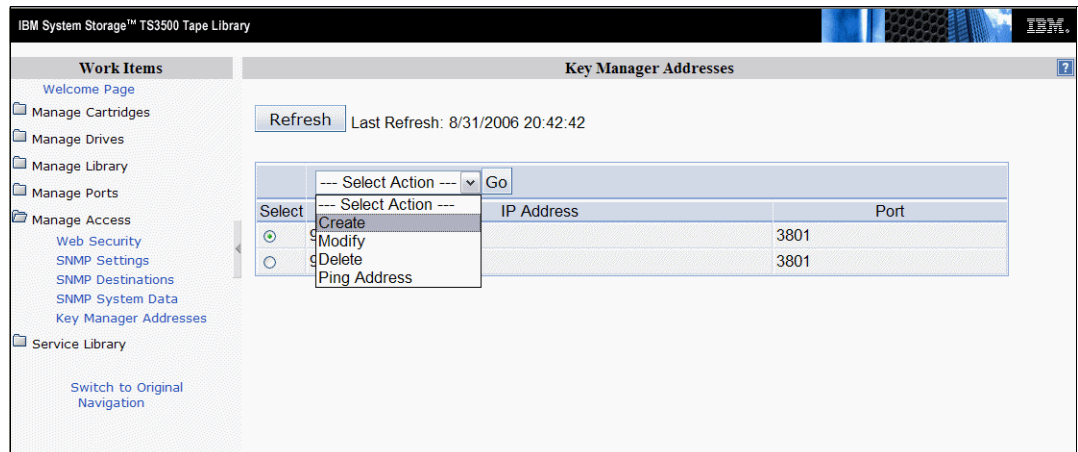


Figure 6-69 Creating a key manager address

4. The Create Key Manager Address window opens. Enter the IP address (Port field must be prefilled) and click **Apply**, as shown in Figure 6-70.

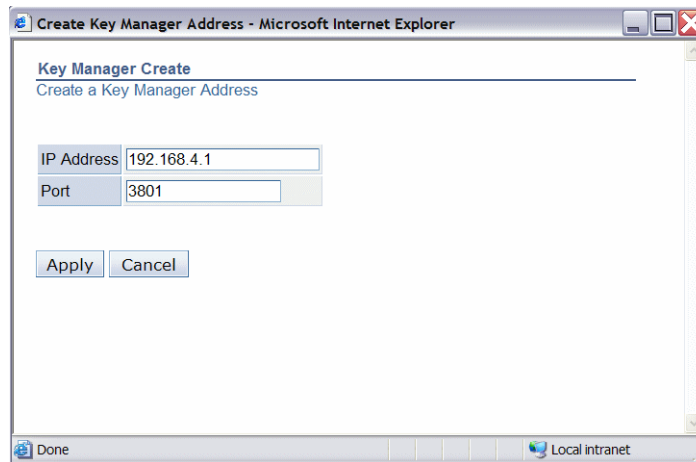


Figure 6-70 Key manager IP address

5. A confirmation window is displayed to confirm that the key manager IP address is added successfully (Figure 6-71).

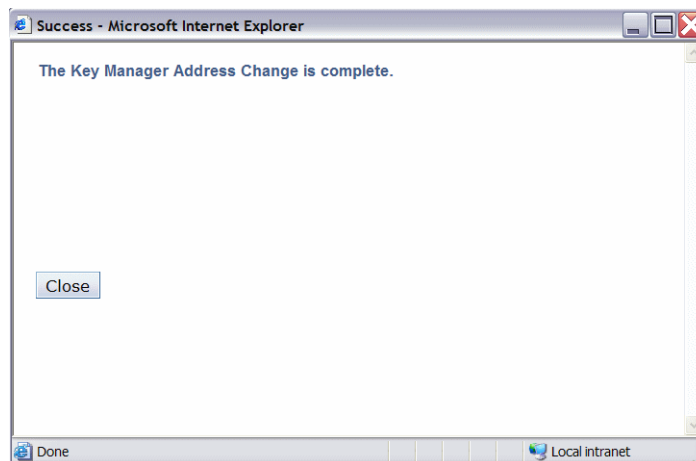


Figure 6-71 Key manager added



6. To test the connection between the TS3500 tape library system and the keystore, select the key manager address and choose **Ping Address** in the Select Action menu, and click **Go** (Figure 6-72).

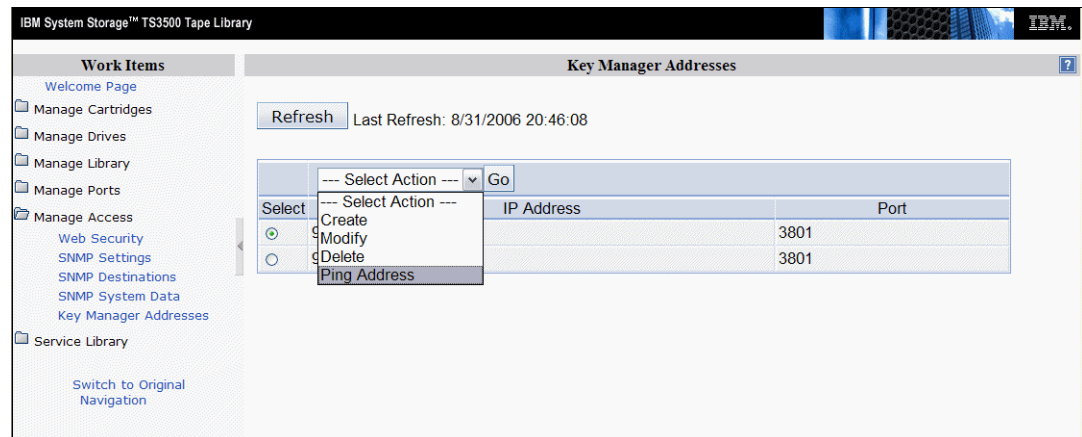


Figure 6-72 Verifying key manager connection

7. If the connection succeeds, a confirmation window is displayed (Figure 6-73).

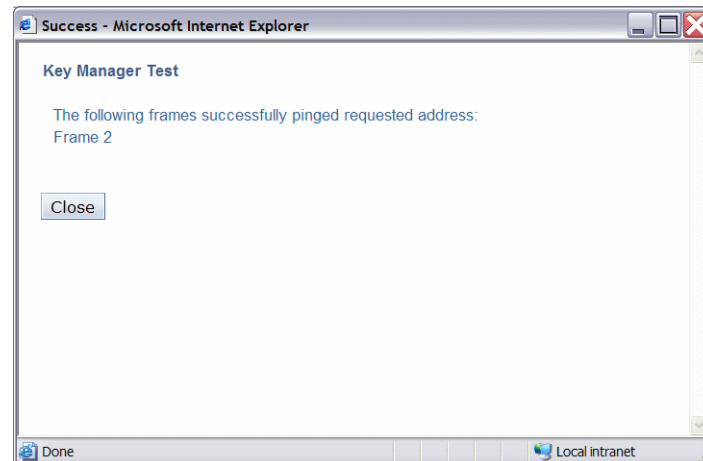


Figure 6-73 Verification of key manager connection successful

## 6.7.2 Enabling your tape drive for encryption

Perform the following tasks:

1. In the left panel, select **Manage Library** → **By Logical Library**. This lists the logical libraries that have been defined in the TS3500 tape library. The last column shows encryption methods in use (Figure 6-74).

IBM System Storage™ TS3500 Tape Library

Work Items: Welcome Page, Manage Cartridges, Manage Drives, **Manage Library** (by Frame, **by Logical Library**, Accessor, Disable ALMS, Virtual IO, Date and Time, 6-Character Volser Reportin), Manage Ports, Manage Access, Service Library. [Switch to Original Navigation](#)

Manage Logical Libraries: Refresh Last Refresh: 8/31/2006 20:25:57

Total Logical Libraries: 5

Select	Logical Library	Type	# Drives	# Cartridges	# VIO Slots	Exports	Encryption Method
			Dedicated Shared	Assigned Max.	Assigned Max.		
<input type="checkbox"/>	LTO-2	LTO	8 0	16 571	0 10	Show	N/A
<input type="checkbox"/>	JAG1	3592	6 0	28 359	0 16	Show	N/A
<input type="checkbox"/>	LTO-1	LTO	8 0	16 571	0 10	Show	N/A
<input type="checkbox"/>	LTO-3	LTO	4 0	46 571	0 10	Show	N/A
<input type="checkbox"/>	JAG2e	3592	2 0	11 359	0 255	Show	Library-Managed

Figure 6-74 Managing logical libraries

2. Select a tape that is capable of encryption, and select **Modify Encryption Method** from the Select Action menu. Click **Go** (Figure 6-75).

IBM System Storage™ TS3500 Tape Library

Work Items: Welcome Page, Manage Cartridges (Data Cartridges, Cleaning Cartridges, I/O Station, Cartridge Assignment Policy, Scratch Encryption Policy, Insert Notification), Manage Drives, **Manage Library** (by Frame, by Logical Library, Accessor, Disable ALMS, Virtual IO, Date and Time, 6-Character Volser Reportin), Manage Ports, Manage Access, Service Library. [Switch to Original Navigation](#)

Manage Logical Libraries: Refresh Last Refresh: 8/31/2006 20:25:57

Total Logical Libraries: 5

Select	Logical Library	Type	# Drives	# Cartridges	# VIO Slots	Exports	Encryption Method
			Dedicated Shared	Assigned Max.	Assigned Max.		
<input type="checkbox"/>	LTO-2	LTO	8 0	16 571	0 10	Show	N/A
<input checked="" type="checkbox"/>	JAG1	3592	6 0	28 359	0 16	Show	N/A
<input type="checkbox"/>	LTO-1	LTO	8 0	16 571	0 10	Show	N/A
<input type="checkbox"/>	LTO-3	LTO	4 0	46 571	0 10	Show	N/A
<input type="checkbox"/>	JAG2e	3592	2 0	11 359	0 255	Show	Library-Managed

Modify Encryption Method

Figure 6-75 Modifying encryption method

3. The Encryption method window is displayed (Figure 6-76). Note that the default value is None, and that the four remaining parameters are for IBM Support use only.

**Attention:** Changing these values is *not* recommended.

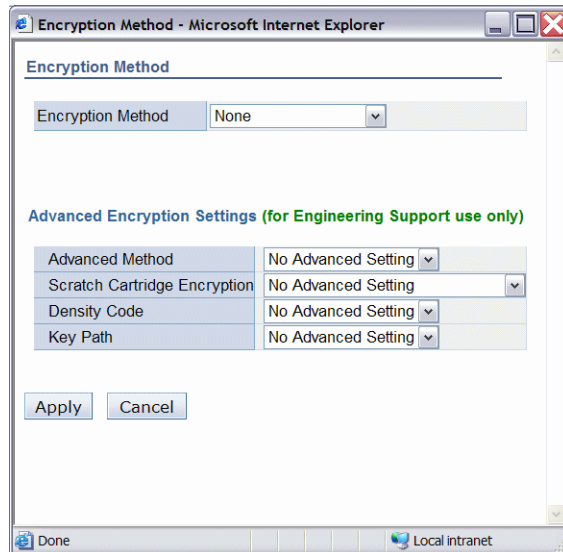


Figure 6-76 Encryption method

4. To change the encryption method, select **Library Managed** in the Encryption Method menu, as shown in Figure 6-77.

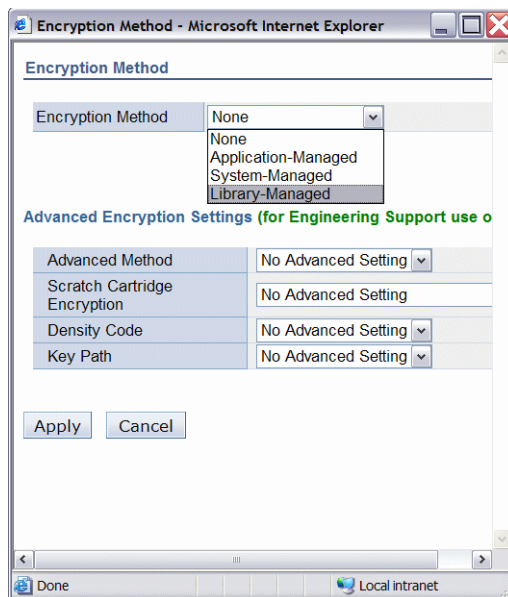


Figure 6-77 Changing encryption method

- As soon as you change the encryption method to Library-Managed, a new field appears on the page, the key manager address selection (Figure 6-78). This is normal when you enable a tape drive for encryption; the tape drive has to know where to get its keys. By using this field, you can point the tape drive to the keystore addresses you selected earlier as described in 6.7.1, “Defining the keystores to be used by the TS3500” on page 184. After specifying the IP addresses of your choice, click **Apply** to confirm.

Encryption Method - Microsoft Internet Explorer

Encryption Method

Library-Managed

Select up to four IP address

Select	IP Address	Port
<input checked="" type="checkbox"/>	9.5.53.92	3801
<input checked="" type="checkbox"/>	9.5.53.94	3801

Advanced Encryption Settings (for Engineering Support use only)

Advanced Method	No Advanced Setting
Scratch Cartridge Encryption	No Advanced Setting
Density Code	No Advanced Setting
Key Path	No Advanced Setting

Apply Cancel

Done Local intranet

Figure 6-78 Library-managed encryption

### 6.7.3 Setting up a scratch encryption policy

In this last stage, define to the TS1120 tape drive the cartridges or “ranges” of cartridges that are eligible for encryption. This policy only applies to scratch tapes because you cannot mix nonencrypted and encrypted data on one cartridge.

**Attention:** This is another point where you must remember not to save the keys to the encrypted media. You must plan for the eligible tapes to be known as encryption-capable. Anyone using these encrypted tapes must understand the restore implications.

To set up a scratch encryption policy, perform the following tasks:

- In the left panel, select **Manage Cartridges** → **Scratch Encryption Policy**. Figure 6-79 on page 191 shows two “Volser” (volume serial) ranges of cartridges that are already defined. Select **Create** from the Select Action menu, and click **Go**.

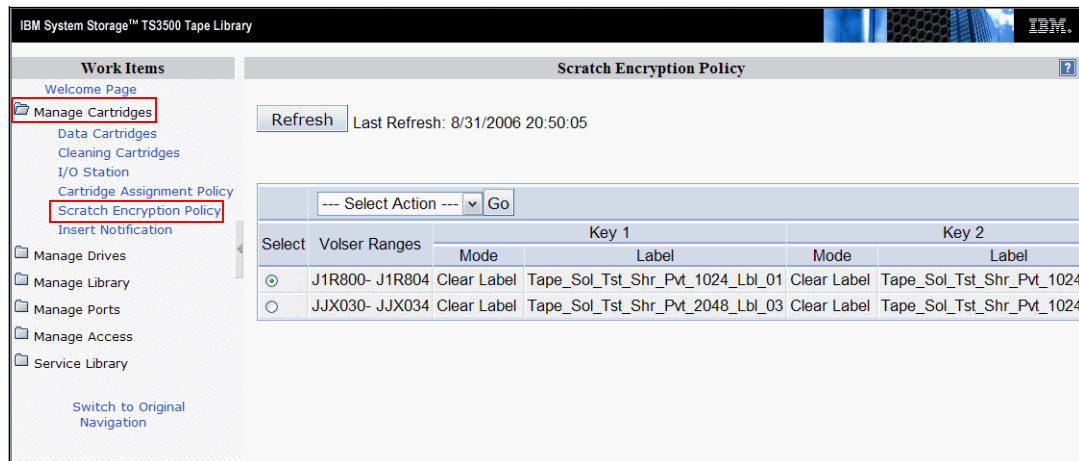


Figure 6-79 Scratch encryption policy

- The Scratch Encryption Policy window is displayed. You can select the **Set All/Other Volsers** check box, or define a range of cartridges to be used for encryption. Each scratch encryption policy requires that you specify two key labels (and key modes). A key label is only a pointer, a common name that enables the tape library and the keystore to identify which keys are to be used for this policy. The same key labels must exist in your keystore. The key mode defines how the keystore identifies the public/private keys used to *encrypt a data key*.

Possible values for key mode are:

- Default Label** The label is configured at the encryption key manager
- Clear Label** The externally encrypted data key (EEDK) that is referenced by the specified key label
- Hash Label** The EEDK that is referenced by a computer value that corresponds to the public key that is referenced by the specified key label

Click **Apply** to encrypt all subsequent scratch tapes in the range ZYX100 - ZYX110 (Figure 6-80).

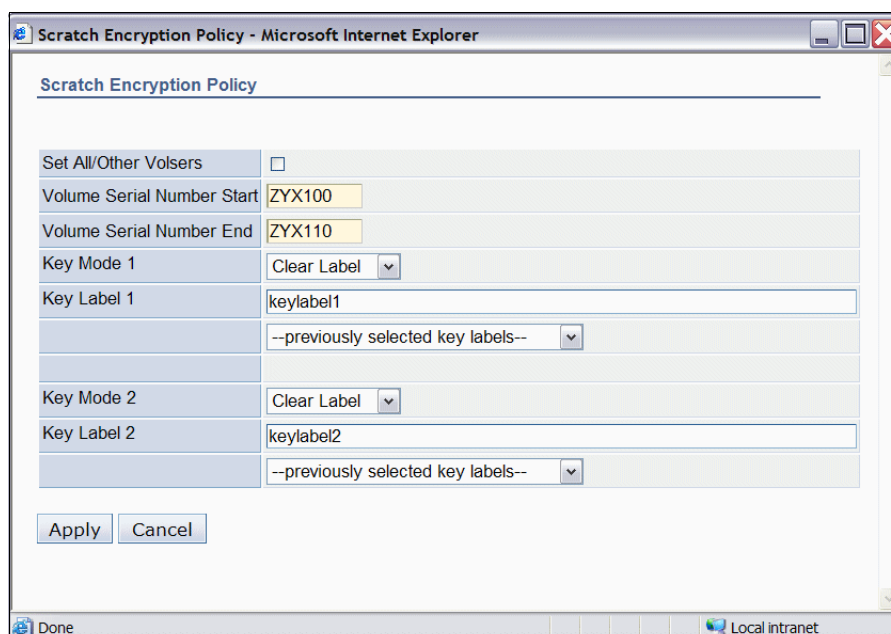


Figure 6-80 Scratch encryption policy definition

- To check whether your cartridges are being encrypted, select **Manage Cartridges** → **Data Cartridges**. Narrow your search by selecting a frame or a logical library. In this example, we selected only the encryption-enabled logical library (Figure 6-81). Click **Search** to display your selection of cartridges.

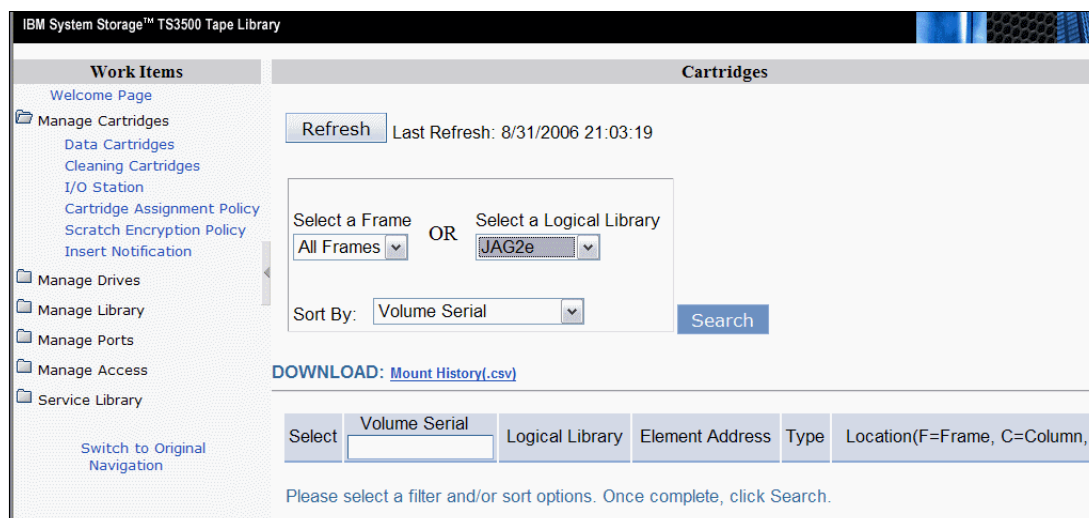


Figure 6-81 Data cartridges

- The last column in the list shows whether a cartridge is encrypted (Figure 6-82).

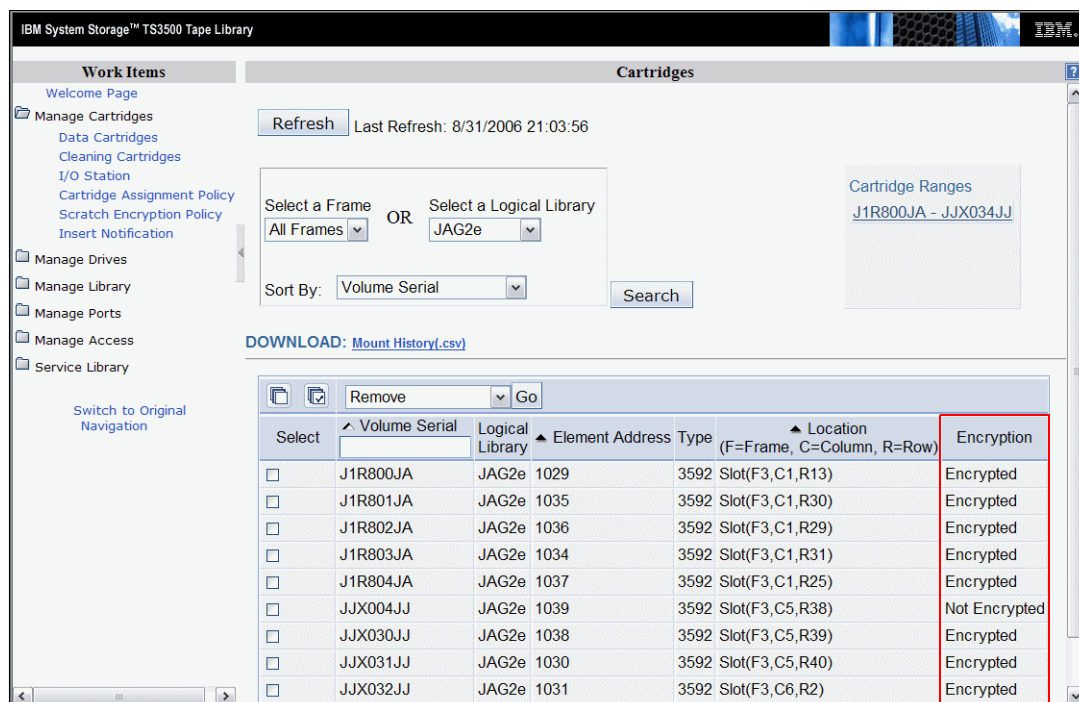


Figure 6-82 Working with data cartridges properties

If you set the Show Density parameter to yes on the library side, you can also tell whether a tape is encrypted by looking at the density type. A nonencrypted tape written on a 3592-E05 drive will show a density of \*FMT3592A1. For an encrypted tape, the density is FMT3592A1E.



**Note:** Remember that the TS3500 library manages the encryption, *not* BRMS or the native i5/OS functions. Although the INZTAP DENSITY(FMT3592A1E) might look like it is working — you receive a message stating that the density has changed — in reality, *the density does not change*.

## 6.7.4 Rekeying an encrypted cartridge for use by another company

When you encrypt a cartridge, it can only be accessed internally. To send your cartridges off to another company and allow them to use the cartridges, rekey the cartridges so that the other company can decrypt the data using a different key. This way, you do not have to give your keys to the other company. Instead, you create a new key pair for use by the other company.

Perform the following tasks:

1. Select **Manage Cartridges** → **Data Cartridges**, define your selection, and click **Search**.
2. Select the tape cartridge you want to rekey, select **ReKey Encryption** from the Select Action menu, and click **Go** (Figure 6-83).

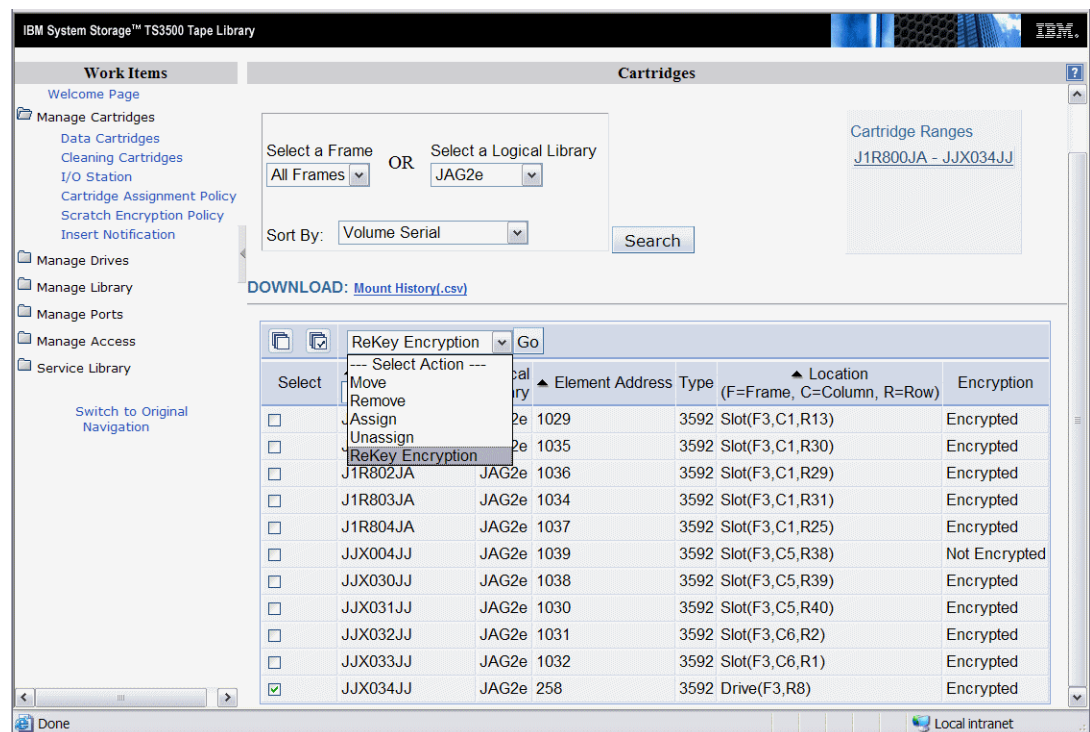


Figure 6-83 Selecting ReKey Encryption

3. The Rekey Encryption window opens. Enter the key modes and labels you want to use to rekey the cartridge, and click **Apply** (Figure 6-84 on page 194).

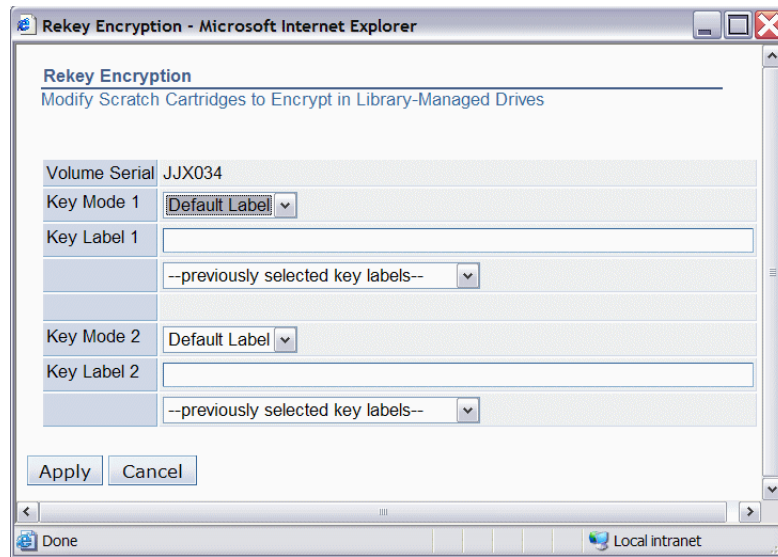


Figure 6-84 Rekey Encryption window



# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this IBM Redbook.

## IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 196. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *IBM System i5, eServer i5, and iSeries Systems Builder IBM i5/OS Version 5 Release 4 - January 2006*, SG24-2155
- ▶ *Logical Partitions on System i5: A Guide to Planning and Configuring LPAR with HMC on System i*, SG24-8000
- ▶ *High-speed Link Loop Architecture for the IBM eServer iSeries Server: OS/400 Version 5 Release 2*, REDP-3652

## Other publications

These publications are also relevant as further information sources:

- ▶ *System i i5/OS and related software: Installing, upgrading, or deleting i5/OS and related software, Version 5 Release 4*, SC41-5120  
<http://publib.boulder.ibm.com/infocenter/iseriess/v5r4/topic/rzahc/rzahc.pdf>
- ▶ *Operations Console Setup*, SC41-5508-02  
<http://www-1.ibm.com/support/docview.wss?uid=publsc41550802>
- ▶ *OS/400 Backup and Recovery V5R4*, SC41-5304  
<http://publib.boulder.ibm.com/infocenter/iseriess/v5r4/topic/books/sc415304.pdf>
- ▶ IBM Encryption Key Manager component for the Java platform, EKM Introduction, Planning, and User's Guide  
<http://www-1.ibm.com/support/docview.wss?uid=ssglS7001618>

## Online resources

These Web sites and URLs are also relevant as further information sources:

- ▶ Dynamic Logical Partitioning  
<http://www.ibm.com/servers/eserver/iseriess/lpar/>
- ▶ Expansion unit conversions in a partitioned environment for 8xx and 270 iSeries server models  
<http://www-1.ibm.com/servers/eserver/iseriess/migration/pdf/LPARexpansionupgradeFINAL.pdf>

- ▶ HSL Rules (High Availability and Clusters)  
<http://www-1.ibm.com/servers/eserver/series/ha/systemdesign.html>
- ▶ IBM CUI Home page  
<http://w3.rchland.ibm.com/projects/WCII/cgi-bin/wciireq.pl>
- ▶ IBM System i5 Benchmark Center  
<http://www.ibm.com/servers/eserver/series/benchmark/cbc/index.html>
- ▶ IBM Systems Workload Estimator  
<http://www-304.ibm.com/jct01004c/systems/support/tools/estimator/index.html>
- ▶ IBM eServer iSeries Information Center  
<http://www.iseries.ibm.com/infocenter>
- ▶ iSeries Memorandum to Users Release -- R530 (Preventive Service Planning)  
[http://www-912.ibm.com/s\\_dir/sline003.nsf/2d3aff1c6b4d6ce086256453000d971e/e8326ca1d7b29aa486256eac005dc19f?OpenDocument](http://www-912.ibm.com/s_dir/sline003.nsf/2d3aff1c6b4d6ce086256453000d971e/e8326ca1d7b29aa486256eac005dc19f?OpenDocument)

## How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

[ibm.com/redbooks](http://ibm.com/redbooks)

## Help from IBM

IBM Support and downloads

[ibm.com/support](http://ibm.com/support)

IBM Global Services

[ibm.com/services](http://ibm.com/services)

# Index

## Symbols

¼-inch 2.5GB 12

¼-inch, 13GB 12

## Numerics

5250 console 91

## A

acceptUnknownDrives 140

ASMI 90

## B

backup and recovery considerations 140

## C

Capacity on Demand 91

CEC 91

## D

data are encrypted by the host 138

define keystore 140

## E

EKM 137

configure 140

server 140

encryption components 139

encryption methods 138

encryption-capable tape drive 138

## F

FC 5592 139

FC 5596 139

FC 9592 139

FC 9596 139

Fibre Channel Disk Adapter 12

Fibre Channel Disk adapter 12

Fibre Channel Tape Adapter 12

Fibre Channel Tape adapter 12

FSIOP 9, 11

## G

graphical user interface 2

## H

Hardware Management Console 3, 90

machine code 93

## I

IBM 5250 emulator 97

IBM Encryption Key Manager 139

IBM Java 140

IBM Software Development Kit 140

IBM TotalStorage TS1120 137

IBM Workload Estimator 3

IBMKeyManagementServer 140

Integrated xSeries Server 12

IPCS 11

## J

Java Runtime Environment 140

JCEKS type keystore 149

## K

key management 150

KeyManagerConfig 140

keystore 140

## L

LPAR Validation Tool 2

LVT 2

## N

Neoware Connection Manager 101

Neoware Thin Client 97

## O

operations console 90

overview of the System Planning Tool 2

## P

planning for tape encryption 140

PTF 92

## R

Redbooks Web site 196

Contact us x

RPQ

847102 12

## S

sample configuration File 140

Sarbanes-Oxley 138

SDK 140

server firmware 92

update policy 93

service partition 92

service processor 91

SPD feature code		5072	8
1360	10	5073	8
1379	10	5074	12
1380	10	5079	12
2609	8	5082	8
2612	9	5083	8
2617	9	6050	8
2618	9	6112	11
2619	9	6141	8
2620	9	6146	11
2621	10	6149	9
2623	9	6153	9
2624	10	6180	8
2626	9	6181	9
2629	8	6325	10
2644	11	6368	10
2654	9	6380	10
2664	12	6385	10
2665	9	6390	10
2666	9	6425	10
2686	8	6485	10
2688	8	6490	10
2695	8	6501	12
2699	9	6502	11
2745	11	6512	11
2748	12	6513	11
2757	12	6517	11
2765	12	6518	11
2766	12	6519	11
2778	12	6532	11
2782	12	6533	11
2790	12	6534	11
2791	12	6605	10
2792	12	6606	10
2799	12	6607	10
2810	9	6616	9
2820	9	6617	9
2892	12	6618	9
2899	12	6650	10
3584-D22	139	6652	10
3584-D23	139	6713	10
3584-L22	139	6714	10
3584-L23	139	6717	12
3592-E05	139	6718	12
4317	12	6806	10
4318	12	6807	10
4482	12	6813	10
4483	12	6817	12
4582	12	6818	12
4583	12	6824	10
4745	11	6906	10
4748	12	6907	10
4778	12	8617	12
5044	8	8664	10
5052	8	8713	10
5055	8	8714	10
5057	8	8817	12
5058	8	9748	12
5065	12	9778	12
5066	12	SSH	90

sysplan file 2  
system plan 2–3

## **T**

tape encryption 137  
Thin Console 97  
    5250 emulation screen 98  
    customization settings 110  
Tivoli Storage Manager 138  
TS1120 137, 139  
TS3500  
    tape library 138  
    system 139  
twinax console 90

## **U**

using EKM and TS1120 tape drive 138

## **W**

WebSM 90  
Workload Estimator 3













# IBM eServer iSeries Migration

## A Guide to Upgrades and Migrations to IBM System i5



**Understand the considerations for upgrades to IBM System i5 in i5/OS V5R4**

**Learn how TS1120 hardware-based tape encryption works with i5/OS**

**Review Thin Console support for low-end System i5 without an HMC**

Planning an upgrade from an existing IBM AS/400e or IBM eServer iSeries server to a new model IBM System i5 can range from a simple disk migration to a complex task involving many components and OS upgrade steps. This IBM Redbook discusses the various topics that are involved in migrating to the new Peripheral Component Interconnect-X (PCI-X), and IBM POWER5 processor technology. We include upgrade scenarios to assist your planning.

IBM i5/OS V5R4 contains additional components, functions, and features, which this book discusses. The new features include the new Thin Console support for the IBM System i5 low-end platform. This book also discusses the new hardware-based tape encryption available with i5/OS V5R4 and the IBM TotalStorage TS1120 tape drive.

Whether you are an IBM Field Technical Support Specialist, business partner, or client, this book offers the guidance to plan your upgrade or migration to a new IBM System i5 environment.

### **INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION**

### **BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:**  
[ibm.com/redbooks](http://ibm.com/redbooks)